

---

# AWS Config

## Developer Guide



## **AWS Config: Developer Guide**

Copyright © Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

## Table of Contents

What Is AWS Config? .....	1
Ways to Use AWS Config .....	1
Resource Administration .....	1
Auditing and Compliance .....	1
Managing and Troubleshooting Configuration Changes .....	2
Security Analysis .....	2
Concepts .....	2
AWS Config .....	3
AWS Config Managed and Custom Rules .....	4
Multi-Account Multi-Region Data Aggregation .....	5
Managing AWS Config .....	5
Control Access to AWS Config .....	6
Partner Solutions .....	6
How AWS Config Works .....	6
Deliver Configuration Items .....	7
Supported Resource Types .....	9
Amazon API Gateway .....	9
Amazon CloudFront .....	9
Amazon CloudWatch .....	10
Amazon DynamoDB .....	10
Amazon Elastic Block Store .....	10
Amazon Elastic Compute Cloud .....	10
Amazon Elastic Container Registry .....	11
Amazon Elastic Container Service .....	12
Amazon Elastic Kubernetes Service .....	12
Amazon Elasticsearch Service .....	12
Amazon Quantum Ledger Database (QLDB) .....	13
Amazon Redshift .....	13
Amazon Relational Database Service .....	13
Amazon S3 Bucket Attributes .....	14
Amazon Simple Notification Service .....	15
Amazon Simple Queue Service .....	15
Amazon Simple Storage Service .....	15
Amazon Virtual Private Cloud .....	15
AWS Auto Scaling .....	16
AWS Certificate Manager .....	17
AWS CloudFormation .....	17
AWS CloudTrail .....	17
AWS CodeBuild .....	17
AWS CodePipeline .....	17
AWS Config .....	18
AWS Elastic Beanstalk .....	18
AWS Identity and Access Management .....	19
AWS Key Management Service .....	19
AWS Lambda Function .....	19
AWS Network Firewall .....	20
AWS Secrets Manager .....	20
AWS Service Catalog .....	20
AWS Shield .....	21
AWS Systems Manager .....	21
AWS WAF .....	21
AWS X-Ray .....	22
Elastic Load Balancing .....	23
Service Limits .....	23

---

Getting Started .....	25
Setting Up AWS Config (Console) .....	25
Setting Up AWS Config (AWS CLI) .....	27
Prerequisites .....	28
Turning on AWS Config .....	30
Verify that AWS Config Is On .....	31
Setting Up AWS Config Rules (Console) .....	33
Viewing the AWS Config Dashboard .....	33
AWS Config .....	35
Region Support .....	35
Components of a Configuration Item .....	37
Record Configurations for Third-Party Resources .....	38
Step 1: Setup Your Development Environment .....	38
Step 2: Model Your Resource .....	38
Step 3: Generate Artifacts .....	40
Step 4: Register Your Resource .....	40
Step 5: Publish Resource Configuration .....	40
Record and Delete a Configuration State for Third-Party Resources Using AWS CLI .....	40
Managing a Configuration State for Third-Party Resources Type Using APIs .....	42
Region Support .....	42
Viewing AWS Resource Configurations and History .....	43
Looking Up Discovered Resources .....	44
Viewing Configuration Details .....	45
Viewing Compliance History .....	49
Delivering Configuration Snapshot .....	51
Managing AWS Config .....	56
Managing the Delivery Channel .....	56
Updating the IAM Role .....	59
Managing the Configuration Recorder .....	60
Selecting Which Resources are Recorded .....	62
Recording Software Configuration for Managed Instances .....	65
Advanced Queries .....	66
Deleting Data .....	80
Example Notifications .....	82
Example Configuration Item Change Notifications .....	83
Example Configuration History Delivery Notification .....	90
Example Configuration Snapshot Delivery Started Notification .....	91
Example Configuration Snapshot Delivery Notification .....	91
Example Compliance Change Notification .....	92
Example Rules Evaluation Started Notification .....	93
Example Oversized Configuration Item Change Notification .....	94
Example Delivery Failed Notification .....	95
AWS Config Rules .....	96
Region Support .....	97
Viewing Configuration Compliance .....	98
Specifying Triggers .....	101
Trigger types .....	101
Example rules with triggers .....	101
Rule evaluations when the configuration recorder is turned off .....	102
Managed Rules .....	102
List of Managed Rules .....	103
Working with Managed Rules .....	191
Creating Managed Rules With AWS CloudFormation Templates .....	192
Custom Rules .....	193
Getting Started with Custom Rules .....	193
Developing a Custom Rule .....	195
Example Functions and Events .....	199

---

---

Managing your AWS Config Rules .....	207
Add, View, Update and Delete Rules (Console) .....	207
View, Update, and Delete Rules (AWS CLI) .....	208
View, Update, and Delete Rules (API) .....	210
Evaluating Your Resources .....	210
Evaluating your Resources (Console) .....	210
Evaluating your Resources (CLI) .....	211
Evaluating your Resources (API) .....	211
Deleting Evaluation Results .....	211
Deleting Evaluating Results (Console) .....	211
Deleting Evaluating Results (CLI) .....	212
Deleting Evaluating Results (API) .....	212
Enabling AWS Config Rules Across all Accounts in Your Organization .....	212
Remediating Resources and Rules .....	213
Prerequisite .....	213
Setting Up Manual Remediation (Console) .....	213
Setting Up Auto Remediation (Console) .....	214
Setting Up and Applying a Remediation Action Remediation Using Rules and Resources (Console) .....	214
Delete Remediation Action (Console) .....	216
Managing Remediation (API) .....	217
Tagging Your Resources .....	217
Restrictions Related to Tagging .....	217
Managing Tags with AWS Config API Actions .....	218
Conformance Packs .....	219
Prerequisites .....	219
Start AWS Config Recording .....	219
Prerequisites for Using a Conformance Pack With Remediation .....	219
Prerequisites for Using a Conformance Pack With One or More AWS Config Rules .....	220
Prerequisites for Organization Conformance Packs .....	220
Region Support .....	220
Process Checks .....	222
Sample Conformance Pack Template for Creating Process Checks .....	223
Include Process Checks Within a Conformance Pack .....	223
Change Compliance Status of a Process Check .....	224
View and Edit the Process Check (Console) .....	225
Conformance Pack Sample Templates .....	225
AWS Control Tower Detective Guardrails Conformance Pack .....	227
Operational Best Practices for ABS CCIG 2.0 Material Workloads .....	227
Operational Best Practices for ABS CCIG 2.0 Standard Workloads .....	313
Operational Best Practices for ACSC Essential 8 .....	372
Operational Best Practices for ACSC ISM .....	398
Operational Best Practices for AI and ML .....	419
Operational Best Practices for Amazon DynamoDB .....	419
Operational Best Practices for Amazon S3 .....	419
Operational Best Practices for APRA CPG 234 .....	420
Operational Best Practices for Asset Management .....	513
Operational Best Practices for AWS Identity And Access Management .....	513
Operational Best Practices for AWS Well-Architected Framework Reliability Pillar .....	514
Operational Best Practices for AWS Well-Architected Framework Security Pillar .....	520
Operational Best Practices for BCP and DR .....	566
Operational Best Practices for BNM RMIIT .....	567
Operational Best Practices for CIS AWS Foundations Benchmark v1.3 Level 1 .....	687
Operational Best Practices for CIS AWS Foundations Benchmark v1.3 Level 2 .....	701
Operational Best Practices for CIS Top 20 .....	719
Operational Best Practices for CMMC Level 1 .....	758
Operational Best Practices for CMMC Level 2 .....	804

---

---

Operational Best Practices for CMMC Level 3 .....	914
Operational Best Practices for CMMC Level 4 .....	1049
Operational Best Practices for CMMC Level 5 .....	1195
Operational Best Practices for Compute Services .....	1360
Operational Best Practices for Data Resiliency .....	1360
Operational Best Practices for Databases Services .....	1361
Operational Best Practices for Data Lakes and Analytics Services .....	1361
Operational Best Practices for EC2 .....	1361
Operational Best Practices for Encryption and Key Management .....	1361
Operational Best Practices for Esquema Nacional de Seguridad (ENS) Low .....	1362
Operational Best Practices for Esquema Nacional de Seguridad (ENS) Medium .....	1436
Operational Best Practices for FDA Title 21 CFR Part 11 .....	1528
Operational Best Practices for FedRAMP(Low) .....	1674
Operational Best Practices for FedRAMP(Moderate) .....	1705
Operational Best Practices for FFIEC .....	1865
Operational Best Practices for HIPAA Security .....	1954
Operational Best Practices for K-ISMS .....	2054
Operational Best Practices for Load Balancing .....	2100
Operational Best Practices for Logging .....	2100
Operational Best Practices for Management and Governance Services .....	2100
Operational Best Practices for MAS Notice 655 .....	2101
Operational Best Practices for MAS TRMG June 2013 .....	2116
Operational Best Practices for Monitoring .....	2260
Operational Best Practices for NBC TRMG .....	2260
Operational Best Practices for NERC CIP .....	2522
Operational Best Practices for NCSC Cloud Security Principles .....	2586
Operational Best Practices for NCSC Cyber Assessment Framework .....	2608
Operational Best Practices for Networking and Content Delivery Services .....	2658
Operational Best Practices for NIST 800-53 rev 4 .....	2658
Operational Best Practices for NIST 800 171 .....	2821
Operational Best Practices for NIST CSF .....	2954
Operational Best Practices for NYDFS 23 .....	3054
Operational Best Practices for PCI DSS 3.2.1 .....	3122
Operational Best Practices for Publicly Accessible Resources .....	3176
Operational Best Practices for RBI Cyber Security Framework for UCBS .....	3177
Operational Best Practices for RBI MD-ITF .....	3194
Operational Best Practices for Security, Identity, and Compliance Services .....	3251
Operational Best Practices for Serverless .....	3251
Operational Best Practices for Storage Services .....	3251
Example Templates with Remediation Action .....	3251
Custom Conformance Pack .....	3252
Viewing Compliance Data in the Conformance Packs Dashboard .....	3252
Navigating the Conformance Packs Main Page .....	3252
Learn more .....	3252
Deploying a Conformance Pack (Console) .....	3252
Deploy a Conformance Pack Using Sample Templates .....	3253
Edit a Conformance Pack .....	3253
Delete a Conformance Pack .....	3254
Deploying a Conformance Pack (AWS CLI) .....	3254
Deploy a Conformance Pack .....	3254
View a Conformance Pack .....	3255
View Conformance Pack Status .....	3255
View Conformance Pack Compliance Status .....	3256
Get Compliance Details for a Specific Conformance Pack .....	3256
Delete a Conformance Pack .....	3257
Managing Conformance Packs (API) .....	3257
Managing Conformance Packs Across all Accounts in Your Organization .....	3257

---

Viewing Compliance History .....	3258
Viewing the Compliance Timeline .....	3259
Querying Compliance History .....	3259
Troubleshooting .....	3260
Multi-Account Multi-Region Data Aggregation .....	3262
Region Support .....	3262
Learn More .....	3264
Viewing Compliance Data in the Aggregator Dashboard .....	3264
Using the Aggregator Dashboard .....	3264
Learn More .....	3266
Setting Up an Aggregator (Console) .....	3266
Add an Aggregator .....	3266
Edit an Aggregator .....	3267
Delete an Aggregator .....	3268
Learn More .....	3266
Setting Up an Aggregator (AWS CLI) .....	3268
Add an Aggregator Using Individual Accounts .....	3269
Add an Aggregator Using AWS Organizations .....	3270
Register a Delegated Administrator .....	3270
View an Aggregator .....	3271
Edit an Aggregator .....	3272
Delete an Aggregator .....	3273
Learn More .....	3266
Authorizing Aggregator Accounts (Console) .....	3274
Add Authorization for Aggregator Accounts and Regions .....	3274
Authorize a Pending Request for an Aggregator Account .....	3275
Delete Authorization for an Existing Aggregator Account .....	3275
Learn More .....	3266
Authorizing Aggregator Accounts (AWS CLI) .....	3275
Add Authorization for Aggregator Accounts and Regions .....	3276
Delete an Authorization Account .....	3276
Learn More .....	3266
Troubleshooting .....	3277
Learn More .....	3266
Security .....	3278
Data Protection .....	3278
Encryption of Data in Transit .....	3279
Encryption of Data in Transit .....	3279
Identity and Access Management .....	3279
Permissions for AWS Config Administration .....	3280
Custom Permissions for AWS Config Users .....	3281
Supported Resource-Level Permissions for AWS Config Rules APIs Actions .....	3287
Permissions for the IAM Role .....	3289
Permissions for the Amazon S3 Bucket .....	3292
Permissions for the KMS Key .....	3294
Permissions for the Amazon SNS Topic .....	3295
Service-Linked AWS Config Rules .....	3297
AWS managed policies .....	3299
AWSConfigServiceRolePolicy .....	3299
AWS_ConfigRole .....	3303
Policy updates .....	3306
Logging and Monitoring .....	3307
Logging AWS Config .....	3307
Monitoring .....	3314
Using Amazon SQS .....	3314
Using Amazon CloudWatch Events .....	3316
Interface Amazon VPC endpoints .....	3318

Availability .....	3318
Create a VPC Endpoint for AWS Config .....	3319
Incident Response .....	3319
Compliance Validation .....	3319
Resilience .....	3320
Infrastructure Security .....	3320
Configuration and Vulnerability Analysis .....	3320
Best Practices .....	3320
AWS Config Resources .....	3321
AWS Software Development Kits for AWS Config .....	3321
FAQs .....	3323
Changes to AWS Config Resource Relationships .....	3323
What is the new change in the AWS Config Resource Relationships? .....	3323
What is a direct and an in-direct relationship with respect to a resource? .....	3323
What is the benefit of this change to AWS Config subscribers? .....	3324
Which resource relationships are being removed? .....	3324
How are the AWS Config managed rules affected? .....	3323
What is the exact impact for custom AWS Config rules that use configuration trigger for these resource types? .....	3323
Should I expect a delay in reporting evaluation results for a managed rule with configuration changes? .....	3323
What is the impact on historical data? Would it still display details about indirect relationships? .....	3323
Is there a change in the output generated by <code>GetResourceConfigHistory</code> API? .....	3323
Is there any change in the resource schema of a Configuration Item? .....	3323
Are there other alternatives to retrieve indirect relationships? .....	3323
Document History .....	3327
Earlier Updates .....	3330
AWS glossary .....	3368

# What Is AWS Config?

AWS Config provides a detailed view of the configuration of AWS resources in your AWS account. This includes how the resources are related to one another and how they were configured in the past so that you can see how the configurations and relationships change over time.

An AWS *resource* is an entity you can work with in AWS, such as an Amazon Elastic Compute Cloud (EC2) instance, an Amazon Elastic Block Store (EBS) volume, a security group, or an Amazon Virtual Private Cloud (VPC). For a complete list of AWS resources supported by AWS Config, see [Supported Resource Types](#) (p. 9).

With AWS Config, you can do the following:

- Evaluate your AWS resource configurations for desired settings.
- Get a snapshot of the current configurations of the supported resources that are associated with your AWS account.
- Retrieve configurations of one or more resources that exist in your account.
- Retrieve historical configurations of one or more resources.
- Receive a notification whenever a resource is created, modified, or deleted.
- View relationships between resources. For example, you might want to find all resources that use a particular security group.

## Ways to Use AWS Config

When you run your applications on AWS, you usually use AWS resources, which you must create and manage collectively. As the demand for your application keeps growing, so does your need to keep track of your AWS resources. AWS Config is designed to help you oversee your application resources in the following scenarios:

### Resource Administration

To exercise better governance over your resource configurations and to detect resource misconfigurations, you need fine-grained visibility into what resources exist and how these resources are configured at any time. You can use AWS Config to notify you whenever resources are created, modified, or deleted without having to monitor these changes by polling the calls made to each resource.

You can use AWS Config rules to evaluate the configuration settings of your AWS resources. When AWS Config detects that a resource violates the conditions in one of your rules, AWS Config flags the resource as noncompliant and sends a notification. AWS Config continuously evaluates your resources as they are created, changed, or deleted.

### Auditing and Compliance

You might be working with data that requires frequent audits to ensure compliance with internal policies and best practices. To demonstrate compliance, you need access to the historical configurations of your resources. This information is provided by AWS Config.

## Managing and Troubleshooting Configuration Changes

When you use multiple AWS resources that depend on one another, a change in the configuration of one resource might have unintended consequences on related resources. With AWS Config, you can view how the resource you intend to modify is related to other resources and assess the impact of your change.

You can also use the historical configurations of your resources provided by AWS Config to troubleshoot issues and to access the last known good configuration of a problem resource.

## Security Analysis

To analyze potential security weaknesses, you need detailed historical information about your AWS resource configurations, such as the AWS Identity and Access Management (IAM) permissions that are granted to your users, or the Amazon EC2 security group rules that control access to your resources.

You can use AWS Config to view the IAM policy that was assigned to an IAM user, group, or role at any time in which AWS Config was recording. This information can help you determine the permissions that belonged to a user at a specific time: for example, you can view whether the user `John Doe` had permission to modify Amazon VPC settings on Jan 1, 2015.

You can also use AWS Config to view the configuration of your EC2 security groups, including the port rules that were open at a specific time. This information can help you determine whether a security group blocked incoming TCP traffic to a specific port.

## Concepts

AWS Config provides a detailed view of the resources associated with your AWS account, including how they are configured, how they are related to one another, and how the configurations and their relationships have changed over time. Let's take a closer look at the concepts of AWS Config.

### Contents

- [AWS Config \(p. 3\)](#)
  - [AWS Resources \(p. 3\)](#)
  - [Configuration History \(p. 3\)](#)
  - [Configuration Items \(p. 3\)](#)
  - [Configuration Recorder \(p. 3\)](#)
  - [Configuration Snapshot \(p. 4\)](#)
  - [Configuration Stream \(p. 4\)](#)
  - [Resource Relationship \(p. 4\)](#)
- [AWS Config Managed and Custom Rules \(p. 4\)](#)
  - [AWS Config Custom Rules \(p. 4\)](#)
- [Multi-Account Multi-Region Data Aggregation \(p. 5\)](#)
  - [Source Account \(p. 5\)](#)
  - [Source Region \(p. 5\)](#)
  - [Aggregator \(p. 5\)](#)
  - [Aggregator Account \(p. 5\)](#)
  - [Authorization \(p. 5\)](#)
- [Managing AWS Config \(p. 5\)](#)

- [AWS Config Console](#) (p. 5)
- [AWS Config CLI](#) (p. 6)
- [AWS Config APIs](#) (p. 6)
- [AWS SDKs](#) (p. 6)
- [Control Access to AWS Config](#) (p. 6)
- [Partner Solutions](#) (p. 6)

## AWS Config

Understanding the basic components of AWS Config will help you track resource inventory and changes and evaluate configurations of your AWS resources.

### AWS Resources

*AWS resources* are entities that you create and manage using the AWS Management Console, the AWS Command Line Interface (CLI), the AWS SDKs, or AWS partner tools. Examples of AWS resources include Amazon EC2 instances, security groups, Amazon VPCs, and Amazon Elastic Block Store. AWS Config refers to each resource using its unique identifier, such as the resource ID or an [Amazon Resource Name \(ARN\)](#). For details, see [Supported Resource Types](#) (p. 9).

### Configuration History

A configuration history is a collection of the configuration items for a given resource over any time period. A configuration history can help you answer questions about, for example, when the resource was first created, how the resource has been configured over the last month, and what configuration changes were introduced yesterday at 9 AM. The configuration history is available to you in multiple formats. AWS Config automatically delivers a configuration history file for each resource type that is being recorded to an Amazon S3 bucket that you specify. You can select a given resource in the AWS Config console and navigate to all previous configuration items for that resource using the timeline. Additionally, you can access the historical configuration items for a resource from the API.

### Configuration Items

A *configuration item* represents a point-in-time view of the various attributes of a supported AWS resource that exists in your account. The components of a configuration item include metadata, attributes, relationships, current configuration, and related events. AWS Config creates a configuration item whenever it detects a change to a resource type that it is recording. For example, if AWS Config is recording Amazon S3 buckets, AWS Config creates a configuration item whenever a bucket is created, updated, or deleted.

For more information, see [Components of a Configuration Item](#) (p. 37).

### Configuration Recorder

The configuration recorder stores the configurations of the supported resources in your account as configuration items. You must first create and then start the configuration recorder before you can start recording. You can stop and restart the configuration recorder at any time. For more information, see [Managing the Configuration Recorder](#) (p. 60).

By default, the configuration recorder records all supported resources in the region where AWS Config is running. You can create a customized configuration recorder that records only the resource types that you specify. For more information, see [Selecting Which Resources AWS Config Records](#) (p. 62).

If you use the AWS Management Console or the CLI to turn on the service, AWS Config automatically creates and starts a configuration recorder for you.

## Configuration Snapshot

A configuration snapshot is a collection of the configuration items for the supported resources that exist in your account. This configuration snapshot is a complete picture of the resources that are being recorded and their configurations. The configuration snapshot can be a useful tool for validating your configuration. For example, you may want to examine the configuration snapshot regularly for resources that are configured incorrectly or that potentially should not exist. The configuration snapshot is available in multiple formats. You can have the configuration snapshot delivered to an Amazon Simple Storage Service (Amazon S3) bucket that you specify. Additionally, you can select a point in time in the AWS Config console and navigate through the snapshot of configuration items using the relationships between the resources.

## Configuration Stream

A configuration stream is an automatically updated list of all configuration items for the resources that AWS Config is recording. Every time a resource is created, modified, or deleted, AWS Config creates a configuration item and adds to the configuration stream. The configuration stream works by using an Amazon Simple Notification Service (Amazon SNS) topic of your choice. The configuration stream is helpful for observing configuration changes as they occur so that you can spot potential problems, generating notifications if certain resources are changed, or updating external systems that need to reflect the configuration of your AWS resources.

## Resource Relationship

AWS Config discovers AWS resources in your account and then creates a map of relationships between AWS resources. For example, a relationship might include an Amazon EBS volume `vol-123ab45d` attached to an Amazon EC2 instance `i-a1b2c3d4` that is associated with security group `sg-ef678hk`.

For more information, see [Supported Resource Types \(p. 9\)](#).

## AWS Config Managed and Custom Rules

An AWS Config rule represents your desired configuration settings for specific AWS resources or for an entire AWS account. AWS Config provides customizable, predefined rules to help you get started. If a resource violates a rule, AWS Config flags the resource and the rule as noncompliant, and AWS Config notifies you through Amazon SNS.

## AWS Config Custom Rules

With AWS Config you can also create custom rules. While AWS Config continuously tracks your resource configuration changes, it checks whether these changes violate any of the conditions in your rules.

After you activate a rule, AWS Config compares your resources to the conditions of the rule. After this initial evaluation, AWS Config continues to run evaluations each time one is triggered. The evaluation triggers are defined as part of the rule, and they can include the following types:

- Configuration changes – AWS Config triggers the evaluation when any resource that matches the rule's scope changes in configuration. The evaluation runs after AWS Config sends a configuration item change notification.
- Periodic – AWS Config runs evaluations for the rule at a frequency that you choose (for example, every 24 hours).

For more information, see [Evaluating Resources with AWS Config Rules \(p. 96\)](#).

## Multi-Account Multi-Region Data Aggregation

Multi-account multi-region data aggregation in AWS Config allows you to aggregate AWS Config configuration and compliance data from multiple accounts and regions into a single account. Multi-account multi-region data aggregation is useful for central IT administrators to monitor compliance for multiple AWS accounts in the enterprise.

### Source Account

A source account is the AWS account from which you want to aggregate AWS Config resource configuration and compliance data. A source account can be an individual account or an organization in AWS Organizations. You can provide source accounts individually or you can retrieve them through AWS Organizations.

### Source Region

A source region is the AWS region from which you want to aggregate AWS Config configuration and compliance data.

### Aggregator

An aggregator is a new resource type in AWS Config that collects AWS Config configuration and compliance data from multiple source accounts and regions. Create an aggregator in the region where you want to see the aggregated AWS Config configuration and compliance data.

### Aggregator Account

An aggregator account is an account where you create an aggregator.

### Authorization

As a source account owner, authorization refers to the permissions you grant to an aggregator account and region to collect your AWS Config configuration and compliance data. Authorization is not required if you are aggregating source accounts that are part of AWS Organizations.

For more information, see topics in [Multi-Account Multi-Region Data Aggregation \(p. 3262\)](#) section.

## Managing AWS Config

### AWS Config Console

You can manage the service using the AWS Config console. The console provides a user interface for performing many AWS Config tasks such as:

- Specifying the types of AWS resources for recording.
- Configuring resources to record, including:
  - Selecting an Amazon S3 bucket.
  - Selecting an Amazon SNS topic.
  - Creating AWS Config role.
- Creating managed rules and custom rules that represent desired configuration settings for specific AWS resources or for an entire AWS account.

- Creating and managing configuration aggregators to aggregate data across multiple accounts and regions.
- Viewing a snapshot of current configurations of the supported resources.
- Viewing relationships between AWS resources.

For more information about the AWS Management Console, see [AWS Management Console](#).

## AWS Config CLI

The AWS Command Line Interface is a unified tool that you can use to interact with AWS Config from the command line. For more information, see the [AWS Command Line Interface User Guide](#). For a complete list of AWS Config CLI commands, see [Available Commands](#).

## AWS Config APIs

In addition to the console and the CLI, you can also use the AWS Config RESTful APIs to program AWS Config directly. For more information, see the [AWS Config API Reference](#).

## AWS SDKs

As an alternative to using the AWS Config API, you can use one of the AWS SDKs. Each SDK consists of libraries and sample code for various programming languages and platforms. The SDKs provide a convenient way to create programmatic access to AWS Config. For example, you can use the SDKs to sign requests cryptographically, manage errors, and retry requests automatically. For more information, see the [Tools for Amazon Web Services](#) page.

## Control Access to AWS Config

AWS Identity and Access Management is a web service that enables Amazon Web Services (AWS) customers to manage users and user permissions. Use IAM to create individual users for anyone who needs access to AWS Config. Create an IAM user for yourself, give that IAM user administrative privileges, and use that IAM user for all of your work. By creating individual IAM users for people accessing your account, you can give each IAM user a unique set of security credentials. You can also grant different permissions to each IAM user. If necessary, you can change or revoke an IAM user's permissions at any time. For more information, see [AWS Identity and Access Management \(p. 3279\)](#).

## Partner Solutions

AWS partners with third-party specialists in logging and analysis to provide solutions that use AWS Config output. For more information, visit the AWS Config detail page at [AWS Config](#).

## How AWS Config Works

When you turn on AWS Config, it first discovers the supported AWS resources that exist in your account and generates a [configuration item \(p. 3\)](#) for each resource.

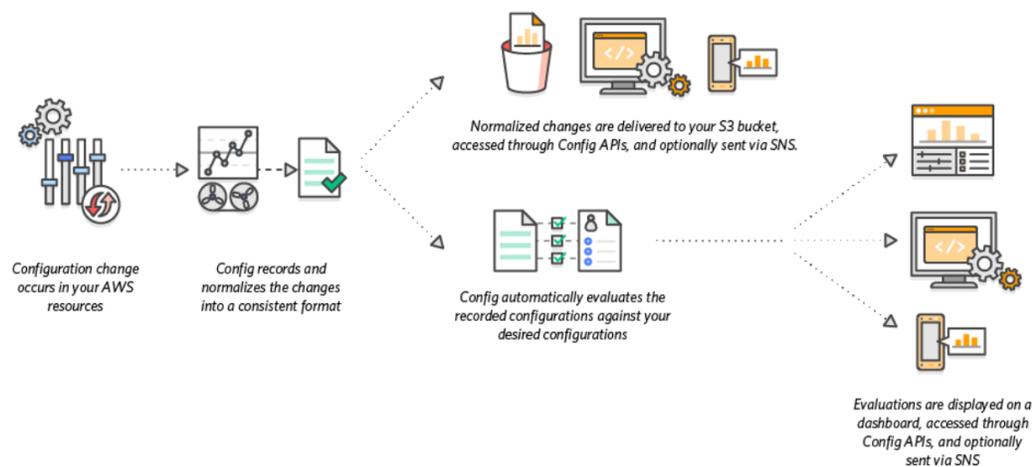
AWS Config also generates configuration items when the configuration of a resource changes, and it maintains historical records of the configuration items of your resources from the time you start the configuration recorder. By default, AWS Config creates configuration items for every supported resource in the region. If you don't want AWS Config to create configuration items for all supported resources, you can specify the resource types that you want it to track.

AWS Config keeps track of all changes to your resources by invoking the Describe or the List API call for each resource in your account. The service uses those same API calls to capture configuration details for all related resources.

For example, removing an egress rule from a VPC security group causes AWS Config to invoke a Describe API call on the security group. AWS Config then invokes a Describe API call on all of the instances associated with the security group. The updated configurations of the security group (the resource) and of each instance (the related resources) are recorded as configuration items and delivered in a configuration stream to an Amazon Simple Storage Service (Amazon S3) bucket.

AWS Config also tracks the configuration changes that were not initiated by the API. AWS Config examines the resource configurations periodically and generates configuration items for the configurations that have changed.

If you are using AWS Config rules, AWS Config continuously evaluates your AWS resource configurations for desired settings. Depending on the rule, AWS Config will evaluate your resources either in response to configuration changes or periodically. Each rule is associated with an AWS Lambda function, which contains the evaluation logic for the rule. When AWS Config evaluates your resources, it invokes the rule's AWS Lambda function. The function returns the compliance status of the evaluated resources. If a resource violates the conditions of a rule, AWS Config flags the resource and the rule as noncompliant. When the compliance status of a resource changes, AWS Config sends a notification to your Amazon SNS topic.



## Deliver Configuration Items

AWS Config can deliver configuration items through one of the following channels:

### Amazon S3 Bucket

AWS Config tracks changes in the configuration of your AWS resources, and it regularly sends updated configuration details to an Amazon S3 bucket that you specify. For each resource type that AWS Config records, it sends a *configuration history file* every six hours. Each configuration history file contains details about the resources that changed in that six-hour period. Each file includes resources of one type, such as Amazon EC2 instances or Amazon EBS volumes. If no configuration changes occur, AWS Config does not send a file.

AWS Config sends a *configuration snapshot* to your Amazon S3 bucket when you use the `deliver-config-snapshot` command with the AWS CLI, or when you use the `DeliverConfigSnapshot` action with the AWS

Config API. A configuration snapshot contains configuration details for all resources that AWS Config records in your AWS account. The configuration history file and configuration snapshot are in JSON format.

**Note**

AWS Config only delivers the configuration history files and configuration snapshots to the specified S3 bucket; AWS Config doesn't modify the lifecycle policies for objects in the S3 bucket. You can use lifecycle policies to specify whether you want to delete or archive objects to Amazon S3 Glacier. For more information, see [Managing Lifecycle Configuration](#) in the *Amazon Simple Storage Service Console User Guide*. You can also see the [Archiving Amazon S3 Data to S3 Glacier](#) blog post.

## Amazon SNS Topic

An Amazon Simple Notification Service (Amazon SNS) topic is a communication channel that Amazon SNS uses to deliver messages (or *notifications*) to subscribing endpoints such as an email address or clients. Other types of Amazon SNS notifications include push notification messages to apps on mobile phones, Short Message Service (SMS) notifications to SMS-enabled mobile phones and smart phones, and HTTP POST requests. For best results, use Amazon SQS as the notification endpoint for the SNS topic and then process the information in the notification programmatically.

AWS Config uses the Amazon SNS topic that you specify to send you notifications. The type of notification that you are receiving is indicated by the value for the `messageType` key in the message body, as in the following example:

```
"messageType": "ConfigurationHistoryDeliveryCompleted"
```

The notifications can be any of the following message types:

`ComplianceChangeNotification`

The compliance type of a resource that AWS Config evaluates has changed. The compliance type indicates whether the resource complies with a specific AWS Config rule, and it is represented by the `ComplianceType` key in the message. The message includes `newEvaluationResult` and `oldEvaluationResult` objects for comparison.

`ConfigRulesEvaluationStarted`

AWS Config started evaluating your rule against the specified resources.

`ConfigurationSnapshotDeliveryStarted`

AWS Config started delivering the configuration snapshot to your Amazon S3 bucket. The name of the Amazon S3 bucket is provided for the `s3Bucket` key in the message.

`ConfigurationSnapshotDeliveryCompleted`

AWS Config successfully delivered the configuration snapshot to your Amazon S3 bucket.

`ConfigurationSnapshotDeliveryFailed`

AWS Config failed to deliver the configuration snapshot to your Amazon S3 bucket.

`ConfigurationHistoryDeliveryCompleted`

AWS Config successfully delivered the configuration history to your Amazon S3 bucket.

`ConfigurationItemChangeNotification`

A resource has been created, deleted, or changed in configuration. This message includes the details of the configuration item that AWS Config creates for this change, and it includes the type of change. These notifications are delivered within minutes of a change and are collectively known as the *configuration stream*.

#### OversizedConfigurationItemChangeNotification

This message type is delivered when a configuration item change notification exceeded the maximum size allowed by Amazon SNS. The message includes a summary of the configuration item. You can view the complete notification in the specified Amazon S3 bucket location.

#### OversizedConfigurationItemChangeDeliveryFailed

AWS Config failed to deliver the oversized configuration item change notification to your Amazon S3 bucket.

For example notifications, see [Notifications that AWS Config Sends to an Amazon SNS topic \(p. 82\)](#).

For more information about Amazon SNS, see the [Amazon Simple Notification Service Developer Guide](#).

## Supported Resource Types

AWS Config supports the following AWS resources types and resource relationships.

### Amazon API Gateway

AWS Service	Resource Type Value	Relationship	Related Resource
API Gateway	AWS::ApiGateway::Stage	is contained in	ApiGateway Rest Api
		is associated with	WAFRegional WebACL
	AWS::ApiGatewayV2::Stage	is contained in	ApiGatewayV2 Api
	AWS::ApiGateway::Resource	contains	ApiGateway Stage
	AWS::ApiGatewayV2::Api	contains	ApiGatewayV2 Stage

To learn more about how AWS Config integrates with Amazon API Gateway, see [Monitoring API Gateway API Configuration with AWS Config](#).

### Amazon CloudFront

AWS Service	Resource Type Value	Relationship	Related Resource
Amazon CloudFront *	AWS::CloudFront::Distribution	is associated with	AWS WAF WebACL
			ACM Certificate
			S3 Bucket
			IAM Server Certificate
	AWS::CloudFront::StreamIngestion	is associated with	AWS WAF WebACL
			ACM Certificate
			S3 Bucket
			IAM Server Certificate

\*AWS Config support for Amazon CloudFront is available only in the US East (N. Virginia) region.

## Amazon CloudWatch

AWS Service	Resource Type Value	Relationship	Related Resource
Amazon CloudWatch	AWS::CloudWatch::Alarm	NA	NA

## Amazon DynamoDB

AWS Service	Resource Type Value	Relationship	Related Resource
Amazon DynamoDB	AWS::DynamoDB::Table	NA	NA

## Amazon Elastic Block Store

AWS Service	Resource Type Value	Relationship	Related Resource
Amazon Elastic Block Store	AWS::EC2::Volume	is attached to	EC2 instance

## Amazon Elastic Compute Cloud

AWS Service	Resource Type Value	Relationship	Related Resource
Amazon Elastic Compute Cloud	AWS::EC2::Host*	contains	EC2 instance
	AWS::EC2::EIP	is attached to	EC2 instance
			Network interface
	AWS::EC2::Instance	contains	EC2 network interface
		is associated with	EC2 security group
		is attached to	Amazon EBS volume
			EC2 Elastic IP (EIP)
		is contained in	EC2 Dedicated host
	AWS::EC2::NetworkInterface	is associated with	Route table
			Subnet
AWS::EC2::NetworkInterface	is associated with	Virtual private cloud (VPC)	
		EC2 security group	
	is attached to	EC2 Elastic IP (EIP)	

AWS Service	Resource Type Value	Relationship	Related Resource
			EC2 instance
		is contained in	Route table
			Subnet
			Virtual private cloud (VPC)
	AWS::EC2::SecurityGroups	is associated with	EC2 instance
			EC2 network interface
			Virtual private cloud (VPC)
	AWS::EC2::NatGateway	is contained in	Virtual private cloud (VPC)
		is contained in	Subnet
	AWS::EC2::EgressOnlyInternetGateway	is attached to	Virtual private cloud (VPC)
	AWS::EC2::FlowLog	NA	NA
	AWS::EC2::VPCEndpoint	is contained in	Virtual private cloud (VPC)
		is attached to	Network interface
		is contained in	Subnet
		is contained in	Route table
	AWS::EC2::VPCEndpoint	is associated with	ElasticLoadBalancingV2 LoadBalancer
	AWS::EC2::VPCPeeringConnection	is associated with	Virtual private cloud (VPC)

\*AWS Config records the configuration details of Dedicated hosts and the instances that you launch on them. As a result, you can use AWS Config as a data source when you report compliance with your server-bound software licenses. For example, you can view the configuration history of an instance and determine which Amazon Machine Image (AMI) it is based on. Then, you can look up the configuration history of the host, which includes details such as the numbers of sockets and cores, to verify that the host complies with the license requirements of the AMI. For more information, see [Tracking Configuration Changes with AWS Config](#) in the *Amazon EC2 User Guide for Linux Instances*.

## Amazon Elastic Container Registry

AWS Service	Resource Type Value	Relationship	Related Resource
Amazon Elastic Container Registry	AWS::ECR::Repository	NA	NA

## Amazon Elastic Container Service

AWS Service	Resource Type Value	Relationship	Related Resource
Amazon Elastic Container Service	AWS::ECS::Cluster	NA	NA
	AWS::ECS::TaskDefinition	NA	ECR Repository
			IAM Role
	AWS::ECS::Service*	NA	ECS Cluster
			ECS TaskDefinition
			IAM role
	AWS::ECS::TaskSet	NA	ECS Cluster
			ECS Service
			ECS TaskDefinition

\*This service currently only support the new Amazon Resource Name (ARN) format. For more information, see [Amazon Resource Names \(ARNs\) and IDs](#) in the ECS developer guide.

Old (not supported): `arn:aws:ecs:region:aws_account_id:service/service-name`

New (supported): `arn:aws:ecs:region:aws_account_id:service/cluster-name/service-name`

## Amazon Elastic Kubernetes Service

AWS Service	Resource Type Value	Relationship	Related Resource
Amazon Elastic Kubernetes Service	AWS::EKS::Cluster	NA	NA

## Amazon Elasticsearch Service

AWS Service	Resource Type Value	Relationship	Related Resource
Amazon Elasticsearch Service	AWS::Elasticsearch::Domain	Associated with	KMS Key
			EC2 security group
			EC2 subnet
			Virtual private cloud (VPC)

## Amazon Quantum Ledger Database (QLDB)

AWS Service	Resource Type Value	Relationship	Related Resource
Amazon QLDB	AWS::QLDB::Ledger	NA	NA

## Amazon Redshift

AWS Service	Resource Type Value	Relationship	Related Resource
Amazon Redshift	AWS::Redshift::Cluster	is associated with	Cluster parameter group
			Cluster security group
			Cluster subnet group
			Security group
			Virtual private cloud (VPC)
	AWS::Redshift::ClusterParameterGroup	NA	NA
	AWS::Redshift::ClusterSecurityGroup	NA	NA
	AWS::Redshift::ClusterSubnetGroup	is associated with	Cluster
AWS::Redshift::ClusterSubnetGroup	is associated with	Virtual private cloud (VPC)	Virtual private cloud (VPC)
			Subnet
AWS::Redshift::ClusterSubnetGroup	is associated with	Virtual private cloud (VPC)	
AWS::Redshift::EventSubscription	NA	NA	

## Amazon Relational Database Service

AWS Service	Resource Type Value	Relationship	Related Resource
Amazon Relational Database Service	AWS::RDS::DBInstance	is associated with	EC2 security group
			RDS DB security group
			RDS DB subnet group
	AWS::RDS::DBSecurityGroup	is associated with	EC2 security group
	AWS::RDS::DBSecurityGroup	is associated with	Virtual private cloud (VPC)

AWS Service	Resource Type Value	Relationship	Related Resource
	AWS::RDS::DBSnapshot	is associated with	Virtual private cloud (VPC)
	AWS::RDS::DBSubnetGroup	is associated with	EC2 security group
			Virtual private cloud (VPC)
	AWS::RDS::EventSubscription	NA	NA
	AWS::RDS::DBCluster	contains	RDS DB instance
		is associated with	RDS DB subnet group
			EC2 security group
	AWS::RDS::DBClusterSnapshot	is associated with	RDS DB cluster
			Virtual private cloud (VPC)

## Amazon S3 Bucket Attributes

AWS Config also records the following attributes for the Amazon S3 bucket resource type.

Attributes	Description
AccelerateConfiguration	Transfer acceleration for data over long distances between your client and a bucket.
BucketAcl	Access control list used to manage access to buckets and objects.
BucketPolicy	Policy that defines the permissions to the bucket.
CrossOriginConfiguration	Allow cross-origin requests to the bucket.
LifecycleConfiguration	Rules that define the lifecycle for objects in your bucket.
LoggingConfiguration	Logging used to track requests for access to the bucket.
NotificationConfiguration	Event notifications used to send alerts or trigger workflows for specified bucket events.
ReplicationConfiguration	Automatic, asynchronous copying of objects across buckets in different AWS Regions.
RequestPaymentConfiguration	Requester pays is enabled.
TaggingConfiguration	Tags added to the bucket to categorize. You can also use tagging to track billing.
WebsiteConfiguration	Static website hosting is enabled for the bucket.
VersioningConfiguration	Versioning is enabled for objects in the bucket.

For more information about the attributes, see [Bucket Configuration Options](#) in the *Amazon Simple Storage Service Developer Guide*.

## Amazon Simple Notification Service

AWS Service	Resource Type Value	Relationship	Related Resource
Amazon Simple Notification Service	AWS::SNS::Topic	NA	NA

## Amazon Simple Queue Service

AWS Service	Resource Type Value	Relationship	Related Resource
Amazon Simple Queue Service	AWS::SQS::Queue	NA	NA

## Amazon Simple Storage Service

AWS Service	Resource Type Value	Relationship	Related Resource
Amazon Simple Storage Service	AWS::S3::Bucket*	NA	NA
	AWS::S3::AccountPublicAccessBlock	NA	NA

\* If you configured AWS Config to record your S3 buckets, and are not receiving configuration change notifications, verify your S3 bucket policies have the required permissions. For more information, see [Managing Permissions for S3 Bucket Recording](#) (p. 3292).

## Amazon Virtual Private Cloud

AWS Service	Resource Type Value	Relationship	Related Resource	
Amazon Virtual Private Cloud	AWS::EC2::CustomerGateway	is attached to	VPN connection	
	AWS::EC2::InternetGateway	is attached to	Virtual private cloud (VPC)	
	AWS::EC2::NetworkACL	NA	NA	
	AWS::EC2::RouteTable		contains	EC2 instance
				EC2 network interface
				Subnet
VPN gateway				
		is contained in	Virtual private cloud (VPC)	

AWS Service	Resource Type Value	Relationship	Related Resource
	AWS::EC2::Subnet	contains	EC2 instance
			EC2 network interface
		is attached to	Network ACL
		is contained in	Route table
			Virtual private cloud (VPC)
	AWS::EC2::VPC	contains	EC2 instance
			EC2 network interface
			Network ACL
			Route table
			Subnet
		is associated with	Security group
	is attached to	Internet gateway	
		VPN gateway	
	AWS::EC2::VPNConnection	is attached to	Customer gateway
			VPN gateway
AWS::EC2::VPNGateway	is attached to	Virtual private cloud (VPC)	
		VPN connection	
	is contained in	Route table	

## AWS Auto Scaling

AWS Service	Resource Type Value	Relationship	Related Resource
Auto Scaling	AWS::AutoScaling::AutoScalingGroup	contains	Amazon EC2 instance
		is associated with	Classic Load Balancer
			Auto Scaling launch configuration
			Subnet
	AWS::AutoScaling::LaunchConfiguration	is associated with	Amazon EC2 security group
	AWS::AutoScaling::ScalingPolicy	is associated with	Auto Scaling group
			Alarm

AWS Service	Resource Type Value	Relationship	Related Resource
	AWS::AutoScaling::ScalingGroup	is associated with	Auto Scaling group

## AWS Certificate Manager

AWS Service	Resource Type Value	Relationship	Related Resource
AWS Certificate Manager	AWS::ACM::Certificate	NA	NA

## AWS CloudFormation

AWS Service	Resource Type Value	Relationship	Related Resource
AWS CloudFormation	AWS::CloudFormation::Stack	contains*	Supported AWS resource types

\*AWS Config records configuration changes to AWS CloudFormation stacks and supported resource types in the stacks. AWS Config does not record configuration changes for resource types in the stack that are not yet supported. Unsupported resource types appear in the supplementary configuration section of the configuration item for the stack.

## AWS CloudTrail

AWS Service	Resource Type Value	Relationship	Related Resource
AWS CloudTrail	AWS::CloudTrail::Trail	NA	NA

## AWS CodeBuild

AWS Service	Resource Type Value	Relationship	Related Resource
AWS CodeBuild	AWS::CodeBuild::Project	is associated with	S3 bucket IAM role

\*To learn more about how AWS Config integrates with AWS CodeBuild, see [Use AWS Config with AWS CodeBuild Sample](#).

## AWS CodePipeline

AWS Service	Resource Type Value	Relationship	Related Resource
AWS CodePipeline	AWS::CodePipeline::Pipeline	is attached to*	S3 bucket

AWS Service	Resource Type Value	Relationship	Related Resource
		is associated with	IAM role
			Code project
			Lambda function
			Cloudformation stack
			ElasticBeanstalk application

\*AWS Config records configuration changes to CodePipeline pipelines and supported resource types in the pipelines. AWS Config does not record configuration changes for resource types in the pipelines that are not yet supported. Unsupported resource types such as CodeCommit repository, CodeDeploy application, ECS cluster, and ECS service appear in the supplementary configuration section of the configuration item for the stack.

## AWS Config

AWS Service	Resource Type Value	Relationship	Related Resource
AWS Config	AWS::Config::ResourceCompliance	is associated with*	All resources*
	AWS::Config::ConformancePackCompliance	NA	NA

\*The relationship between AWS::Config::ResourceCompliance and a related resource depends on how AWS::Config::ResourceCompliance reports compliance for that specific resource type.

**Note**

Recording for the AWS::Config::ConformancePackCompliance resource type is available at no additional charge.

## AWS Elastic Beanstalk

AWS Service	Resource Type Value	Relationship	Related Resource
AWS Elastic Beanstalk	AWS::ElasticBeanstalk::Application	contains	Elastic Beanstalk Application Version
			Elastic Beanstalk Environment
		is associated with	IAM role
	AWS::ElasticBeanstalk::ApplicationVersion	is contained in	Elastic Beanstalk Application
		is associated with	Elastic Beanstalk Environment
			S3 bucket
AWS::ElasticBeanstalk::Environment	is contained in	Elastic Beanstalk Application	

AWS Service	Resource Type Value	Relationship	Related Resource
		is associated with	Elastic Beanstalk Application Version
			IAM role
		contains	CloudFormation Stack

## AWS Identity and Access Management

AWS Service	Resource Type Value	Relationship	Related Resource
AWS Identity and Access Management	AWS::IAM::User <sup>*</sup>	is attached to	IAM group
			IAM customer managed policy
	AWS::IAM::Group <sup>*</sup>	contains	IAM user
			is attached to
	AWS::IAM::Role <sup>*</sup>	is attached to	IAM customer managed policy
	AWS::IAM::Policy	is attached to	IAM user
			IAM group
			IAM role

<sup>\*</sup> AWS Identity and Access Management (IAM) resources are *global resources*. Global resources are not tied to an individual region and can be used in all regions. The configuration details for a global resource are the same in all regions. For more information, see [Selecting Which Resources AWS Config Records](#) (p. 62).

AWS Config includes inline policies with the configuration details that it records.

## AWS Key Management Service

AWS Service	Resource Type Value	Relationship	Related Resource
AWS Key Management Service	AWS::KMS::Key	NA	NA

## AWS Lambda Function

AWS Service	Resource Type Value	Relationship	Related Resource
AWS Lambda Function	AWS::Lambda::Function	is associated with	IAM role

AWS Service	Resource Type Value	Relationship	Related Resource
			EC2 security group
		contains	EC2 subnet

## AWS Network Firewall

AWS Service	Resource Type Value	Relationship	Related Resource
AWS Network Firewall	AWS::NetworkFirewall	is attached to	EC2 Subnet
		is associated with	NetworkFirewall FirewallPolicy
	AWS::NetworkFirewall	is associated with	NetworkFirewall RuleGroup
	AWS::NetworkFirewall	is associated with	NA

AWS Config support for Network Firewall is available only in the US East (N. Virginia), Europe (Ireland) and US West (Oregon) regions.

## AWS Secrets Manager

AWS Service	Resource Type Value	Relationship	Related Resource
AWS SecretsManager	AWS::SecretsManager	is associated with	Lambda function
		is associated with	KMS Key

## AWS Service Catalog

AWS Service	Resource Type Value	Relationship	Related Resource
AWS Service Catalog	AWS::ServiceCatalog	contains	Portfolio
		is associated with	CloudFormationProvisionedProduct
	AWS::ServiceCatalog	is associated with	Portfolio
			CloudFormationProduct
			CloudFormationStack
AWS::ServiceCatalog	contains	CloudFormationProduct	

## AWS Shield

AWS Service	Resource Type Value	Relationship	Related Resource
AWS Shield*	AWS::Shield::Protection	is associated with	Amazon CloudFront distribution
	AWS::ShieldRegional::Protection	is associated with	EC2 EIP
		is associated with	ElasticLoadBalancing Balancer
		is associated with	ElasticLoadBalancingV2 LoadBalancer

\* AWS Config support for AWS::Shield::Protection is available only in the US East (N. Virginia) region. The AWS::ShieldRegional::Protection is available in all regions where AWS Shield is supported.

## AWS Systems Manager

AWS Service	Resource Type Value	Relationship	Related Resource
AWS Systems Manager	AWS::SSM::ManagedInstance	is associated with*	EC2 instance
	AWS::SSM::PatchCompliance	is associated with	Managed Instance Inventory
	AWS::SSM::Association	is associated with	Managed Instance Inventory
	AWS::SSM::FileData	is associated with	Managed Instance Inventory

\* To learn more about managed instance inventory, see [Recording Software Configuration for Managed Instances](#) (p. 65).

## AWS WAF

AWS Service	Resource Type Value	Relationship	Related Resource
AWS WAF*	AWS::WAF::RateBasedRule	NA	NA
	AWS::WAF::Rule	NA	NA
	AWS::WAF::WebACL	is associated with	WAF Rule
			WAF rate based rule
			WAF Rulegroup
AWS::WAF::RuleGroup	is associated with	WAF Rule	

AWS Service	Resource Type Value	Relationship	Related Resource
	AWS::WAFRegional::RateBasedRule	NA	NA
	AWS::WAFRegional::Rule	NA	NA
	AWS::WAFRegional::WebACL	is associated with	ElasticLoadBalancingV2 LoadBalancer
			WAFRegional Rule
			WAFRegional rate based rule
			WAFRegional Rulegroup
	AWS::WAFRegional::RuleGroup	is associated with	WAFRegional Rule

\*The AWS WAF resource type values are available only in the US East (N. Virginia) Region. The AWS::WAFRegional::RateBasedRule, AWS::WAFRegional::Rule, AWS::WAFRegional::WebACL, and AWS::WAFRegional::RuleGroup are available in all regions where AWS WAF is supported.

AWS Service	Resource Type Value	Relationship	Related Resource
AWS WAFv2*	AWS::WAFv2::WebACL	is associated with	ElasticLoadBalancingV2 LoadBalancer
			ApiGateway Stage
			WAFv2 IPSet
			WAFv2 RegexPatternSet
			WAFv2 RuleGroup
			WAFv2 ManagedRuleSet
	AWS::WAFv2::RuleGroup	is associated with	WAFv2 IPSet
			WAFv2 RegexPatternSet
	AWS::WAFv2::ManagedRuleSet	is associated with	WAFv2 RuleGroup

\*The AWS WAFv2 resource type values are available in all the AWS Regions where AWS WAFv2 is supported.

## AWS X-Ray

AWS Service	Resource Type Value	Relationship	Related Resource
AWS X-Ray	AWS::XRay::EncryptionConfig	NA	NA

## Elastic Load Balancing

AWS Service	Resource Type Value	Relationship	Related Resource
Elastic Load Balancing	Application Load Balancer	is associated with	EC2 security group
		is attached to	Subnet
	AWS::ElasticLoadBalancingV2::LoadBalancer	is contained in	Virtual private cloud (VPC)
	Classic Load Balancer	is associated with	EC2 security group
		is attached to	Subnet
	AWS::ElasticLoadBalancing::LoadBalancer	is contained in	Virtual private cloud (VPC)
Network Load Balancer	NA	NA	
AWS::ElasticLoadBalancingV2::LoadBalancer			

## Service Limits

The following table describes limits within AWS Config. Unless noted otherwise, the quotas can be increased upon request. You can [request a quota increase](#).

For information about other limits in AWS, see [AWS Service Limits](#).

### AWS Config Service Limits

Description	Limit Value	Can be increased
Maximum number of AWS Config Rules per Region per account	250	Yes
Maximum number of configuration aggregators	50	Yes
Maximum number of accounts in an aggregator	10000	No
Maximum number of accounts added or deleted per week for all aggregators	1000	Yes
Maximum number of Tags	50	No
Maximum number of saved queries in a single account and a Region	300	Yes

### Single Account Conformance Packs

Description	Limit Value	Can be increased
Maximum number of conformance packs per account	50	No
Maximum number of AWS Config Rules per conformance pack	100	No
Maximum number of AWS Config Rules per account across all conformance packs	150	No

### Organization Conformance Packs

Description	Limit Value	Can be increased
Maximum number of conformance packs per organization	50	No
Maximum AWS Config Rules per organization conformance pack	25	No
Maximum number of AWS Config Rules per account across all organization conformance packs	150	No

### Organization Config Rules

Description	Limit Value	Can be increased
Maximum number of organization AWS Config rules per organization	150	No

# Getting Started with AWS Config

When you sign up for AWS, your account has access to all AWS services. You pay only for the services that you use.

If you do not have an AWS account, complete the following steps to create one.

## To sign up for an AWS account

1. Open <https://portal.aws.amazon.com/billing/signup>.
2. Follow the online instructions.

Part of the sign-up procedure involves receiving a phone call and entering a verification code on the phone keypad.

After you sign up for an AWS account, you can get started with AWS Config with the AWS Management Console, AWS CLI, or the AWS SDKs. Use the console for a quick and streamlined process.

When you set up AWS Config, you can complete the following:

- Specify the resource types that you want AWS Config to record.
- Set up an Amazon S3 bucket to receive a configuration snapshot on request and configuration history.
- Set up an Amazon SNS topic to send configuration stream notifications.
- Grant AWS Config the permissions it needs to access the Amazon S3 bucket and the SNS topic.
- Specify the rules that you want AWS Config to use to evaluate compliance information for the recorded resource types.

For more information about using the AWS CLI, see [Setting Up AWS Config with the AWS CLI \(p. 27\)](#).

For more information about using the AWS SDKs, see [AWS Software Development Kits for AWS Config \(p. 3321\)](#).

## Topics

- [Setting Up AWS Config with the Console \(p. 25\)](#)
- [Setting Up AWS Config with the AWS CLI \(p. 27\)](#)
- [Setting Up AWS Config Rules with the Console \(p. 33\)](#)
- [Viewing the AWS Config Dashboard \(p. 33\)](#)

## Setting Up AWS Config with the Console

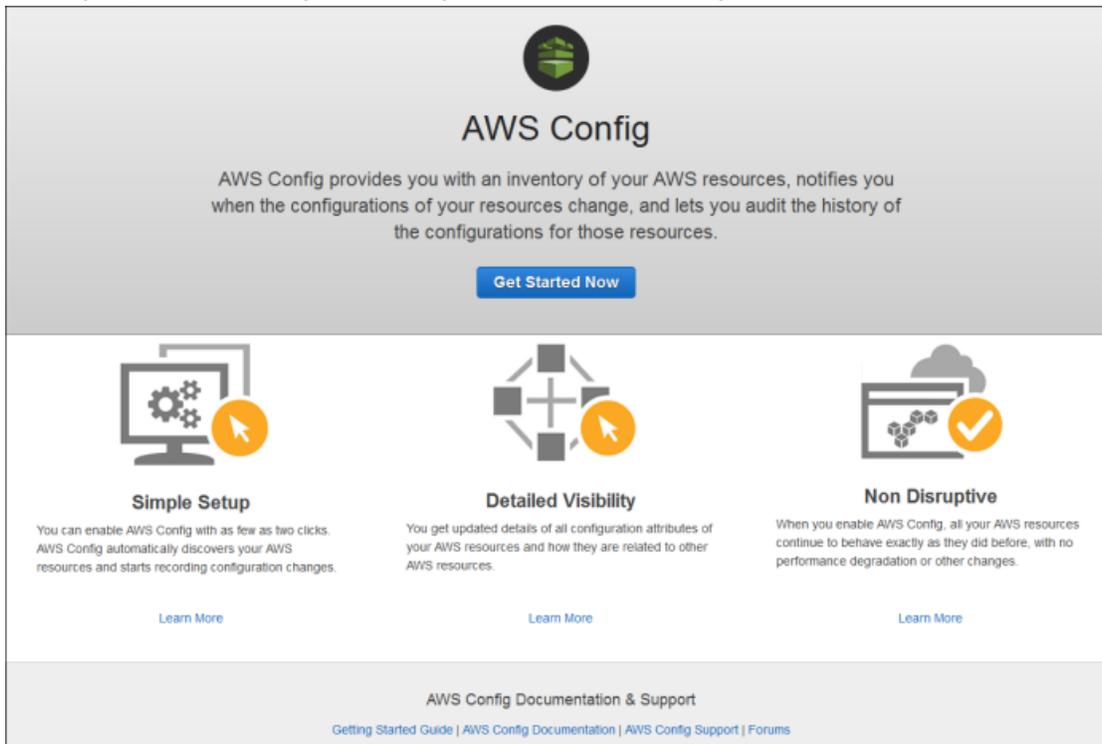
You can use the AWS Management Console to get started with AWS Config to do the following:

- Specify the resource types you want AWS Config to record.
- Set up Amazon SNS to notify you of configuration changes.
- Specify an Amazon S3 bucket to receive configuration information.
- Add AWS Config managed rules to evaluate the resource types.

If you are using AWS Config for the first time or configuring AWS Config for a new region, you can choose managed rules to evaluate resource configurations. For regions that support AWS Config and AWS Config Rules, see [AWS Config Regions and Endpoints](#) in the *Amazon Web Services General Reference*.

## To set up AWS Config with the console

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. If this is the first time you are opening the AWS Config console or you are setting up AWS Config in a new region, the AWS Config console page looks like the following:



3. Choose **Get Started Now**.
  4. On the **Settings** page, for **Resource types to record**, specify all the resource types you want AWS Config to record. These resource types are AWS resources or third-party resources or custom resources.
    - **All resources** – AWS Config records all supported resources with the following options:
      - **Record all resources supported in this region** – AWS Config records configuration changes for supported AWS resource types as well as third-party resource types registered in AWS CloudFormation registry. AWS Config automatically starts recording new supported AWS resource types. It also automatically starts recording third-party resource types that are managed (i.e. created/updated/deleted) through AWS CloudFormation.
      - **Include global resources** – AWS Config includes supported types of global resources with the resources that it records (for example, IAM resources). When AWS Config adds support for a new global resource type, AWS Config automatically starts recording resources of that type.
    - **Specific types** – AWS Config records configuration changes for only the resource types that you specify.
- For more information about these options, see [Selecting Which Resources AWS Config Records](#) (p. 62).
5. For **Amazon S3 Bucket**, choose the Amazon S3 bucket to which AWS Config sends configuration history and configuration snapshot files:
    - **Create a new bucket** – For **Bucket Name**, type a name for your Amazon S3 bucket.

The name that you type must be unique across all existing bucket names in Amazon S3. One way to help ensure uniqueness is to include a prefix; for example, the name of your organization. You can't change the bucket name after it is created. For more information, see [Bucket Restrictions and Limitations](#) in the *Amazon Simple Storage Service Developer Guide*.

- **Choose a bucket from your account** – For **Bucket Name**, choose your preferred bucket.
- **Choose a bucket from another account** – For **Bucket Name**, type the bucket name.

If you choose a bucket from another account, that bucket must have policies that grant access permissions to AWS Config. For more information, see [Permissions for the Amazon S3 Bucket](#) (p. 3292).

6. For **Amazon SNS Topic**, choose whether AWS Config streams information by selecting the **Stream configuration changes and notifications to an Amazon SNS topic**. AWS Config sends notifications such as configuration history delivery, configuration snapshot delivery, and compliance.
7. If you chose to have AWS Config stream to an Amazon SNS topic, choose the target topic:
  - **Create a new topic** – For **Topic Name**, type a name for your SNS topic.
  - **Choose a topic from your account** – For **Topic Name**, select your preferred topic.
  - **Choose a topic from another account** – For **Topic ARN**, type the Amazon Resource Name (ARN) of the topic. If you choose a topic from another account, the topic must have policies that grant access permissions to AWS Config. For more information, see [Permissions for the Amazon SNS Topic](#) (p. 3295).

**Note**

The Amazon SNS topic must exist in the same region as the region in which you set up AWS Config.

8. For **AWS Config role**, choose the IAM role that grants AWS Config permission to record configuration information and send this information to Amazon S3 and Amazon SNS:
  - **Create a role** – AWS Config creates a role that has the required permissions. For **Role name**, you can customize the name that AWS Config creates.
  - **Choose a role from your account** – For **Role name**, choose an IAM role in your account. AWS Config will attach the required policies. For more information, see [Permissions for the IAM Role Assigned to AWS Config](#) (p. 3289).

**Note**

Check the box if you want to use the IAM role as is. AWS Config will not attach policies to the role.

9. If you are setting up AWS Config in a region that supports rules, choose **Next**. See [Setting Up AWS Config Rules with the Console](#) (p. 33).

Otherwise, choose **Save**. AWS Config displays the **Resource inventory** page.

For information about looking up the existing resources in your account and understanding the configurations of your resources, see [View, and Manage Your AWS Resources](#) (p. 43).

You can also use Amazon Simple Queue Service to monitor AWS resources programmatically. For more information, see [Monitoring AWS Resource Changes with Amazon SQS](#) (p. 3314).

## Setting Up AWS Config with the AWS CLI

You can use the AWS Command Line Interface to control and automate the services from AWS.

For more information about the AWS CLI and for instructions on installing the AWS CLI tools, see the following in the *AWS Command Line Interface User Guide*.

- [AWS Command Line Interface User Guide](#)
- [Getting Set Up with the AWS Command Line Interface](#)

See the following topics to set up AWS Config with the AWS CLI. After you set up AWS Config, you can add rules to evaluate the resource types in your account. For more information about setting up rules with AWS Config, see [View, Update, and Delete Rules \(AWS CLI\)](#) (p. 208).

#### Topics

- [Prerequisites](#) (p. 28)
- [Turning on AWS Config](#) (p. 30)
- [Verify that AWS Config Is On](#) (p. 31)

## Prerequisites

Follow this procedure to create an Amazon S3 bucket, an Amazon SNS topic, and an IAM role with attached policies. You can then use the AWS CLI to specify the bucket, topic, and role for AWS Config.

#### Contents

- [Creating an Amazon S3 Bucket](#) (p. 28)
- [Creating an Amazon SNS Topic](#) (p. 29)
- [Creating an IAM Role](#) (p. 29)

## Creating an Amazon S3 Bucket

If you already have an Amazon S3 bucket in your account and want to use it, skip this step and go to [Creating an Amazon SNS Topic](#) (p. 29).

To create an Amazon S3 bucket with the AWS CLI, use the [create-bucket](#) command.

#### To create an Amazon S3 bucket with the console

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. Choose **Actions** and then choose **Create Bucket**.
3. For the **Bucket Name**, type a name for your Amazon S3 bucket, such as *my-config-bucket*.

#### Note

Make sure the bucket name you choose is unique across all existing bucket names in Amazon S3. You cannot change the name of a bucket after it is created. For more information on bucket naming rules and conventions, see [Bucket restrictions and Limitations](#) in the *Amazon Simple Storage Service Developer Guide*.

4. Choose **Create**.

#### Note

You can also use an Amazon S3 bucket from a different account, but you may need to create a policy for the bucket that grants access permissions to AWS Config. For information on granting permissions to an Amazon S3 bucket, see [Permissions for the Amazon S3 Bucket](#) (p. 3292), and then go to [Creating an Amazon SNS Topic](#) (p. 29).

## Creating an Amazon SNS Topic

If you already have an Amazon SNS topic in your account and want to use it, skip this step and go to [Creating an IAM Role \(p. 29\)](#).

To create an Amazon SNS topic with the AWS CLI, use the `create-topic` command.

### To create an Amazon SNS topic with the console

1. Sign in to the AWS Management Console and open the Amazon SNS console at <https://console.aws.amazon.com/sns/v3/home>.
2. Choose **Create New Topic**.
3. For **Topic Name**, type a name for your SNS topic, such as *my-config-notice*.
4. Choose **Create Topic**.

The new topic appears in the **Topic Details** page. Copy the **Topic ARN** for the next task.

For more information, see [ARN Format](#) in the *AWS General Reference*.

To receive notifications from AWS Config, you must subscribe an email address to the topic.

### To subscribe an email address to the SNS topic

1. In the Amazon SNS console, choose **Subscriptions** in the navigation pane.
2. On the **Subscriptions** page, choose **Create Subscription**.
3. For **Topic ARN**, paste the topic ARN you copied in the previous task.
4. For **Protocol**, choose **Email**.
5. For **Endpoint**, type an email address that you can use to receive the notification and then choose **Subscribe**.
6. Go to your email application and open the message from **AWS Notifications**. Choose the link to confirm your subscription.

Your web browser displays a confirmation response from Amazon SNS. Amazon SNS is now configured to receive notifications and send the notification as an email to the specified email address.

#### Note

You can also use an Amazon SNS topic in a different account, but in that case you might need to create a policy for topic that grants access permissions to AWS Config. For information on granting permissions to an Amazon SNS topic, see [Permissions for the Amazon SNS Topic \(p. 3295\)](#) and then go to [Creating an IAM Role \(p. 29\)](#).

## Creating an IAM Role

You can use the IAM console to create an IAM role that grants AWS Config permissions to access your Amazon S3 bucket, access your Amazon SNS topic, and get configuration details for supported AWS resources. After you create the IAM role, you will create and attach policies to the role.

To create an IAM role with the AWS CLI, use the `create-role` command. You can then attach a policy to the role with the `attach-role-policy` command.

### To create an IAM role with the console

1. Sign in to the AWS Management Console and open the IAM console at <https://console.aws.amazon.com/iam/>.

2. In the IAM console, choose **Roles** in the navigation pane, and choose **Create New Role**.
3. For **Role Name**, type a name that describes the purpose of this role. Role names must be unique within your AWS account. Because various entities might reference the role, you cannot edit the name of the role after you create it.

Choose **Next Step**.

4. Choose **AWS Service Roles**, and then choose **Select for AWS Config**.
5. On the **Attach Policy** page, select **AWS\_ConfigRole**. This AWS managed policy grants AWS Config permission to get configuration details for supported AWS resources. Then, choose **Next Step**.
6. On the **Review** page, review the details about your role, and choose **Create Role**.
7. On the **Roles** page, choose the role that you created to open its details page.

You will expand the permissions in the role by creating inline policies that allow AWS Config to access your Amazon S3 bucket and your Amazon SNS topic.

### To create an inline policy that grants AWS Config permission to access your Amazon S3 bucket

1. In the **Permissions** section, expand the **Inline Policies** section, and choose **click here**.
2. Choose **Custom Policy**, and choose **Select**.
3. For **Policy Name**, type a name for your inline policy.
4. Copy the example Amazon S3 bucket policy in [IAM Role Policy for Amazon S3 Bucket \(p. 3290\)](#) and paste it in the **Policy Document** editor.

#### Important

Before you proceed to the next step, replace the following values in the policy. If you do not replace the values, your policy will fail.

- *myBucketName* – Replace with the name of your Amazon S3 bucket.
- *prefix* – Replace with your own prefix or leave blank by removing the trailing '/'.
- *myAccountID-WithoutHyphens* – Replace with your AWS account ID.

5. Choose **Apply Policy**.

### To create an inline policy that grants AWS Config permissions to deliver notifications to your Amazon SNS topic

1. In the **Permissions** section, expand the **Inline Policies** section, and choose **click here**.
2. Choose **Custom Policy**, and choose **Select**.
3. For **Policy Name**, type a name for your inline policy.
4. Copy the Amazon SNS topic example policy in [IAM Role Policy for Amazon SNS Topic \(p. 3291\)](#) and paste it in the **Policy Document** editor.

#### Important

Before you proceed to the next step, replace *arn:aws:sns:region:account-id:myTopic* with the ARN you saved when you created your Amazon SNS topic.

5. Choose **Apply Policy**.

## Turning on AWS Config

You can use the AWS CLI to turn on AWS Config with the `subscribe` command and a few parameters.

You can use the `subscribe` command to have AWS Config start recording configurations of all supported AWS resources in your account. The `subscribe` command creates a configuration recorder, a delivery channel using a specified Amazon S3 bucket and Amazon SNS topic, and starts recording the configuration items. You can have one configuration recorder and one delivery channel per region in your account.

To turn on AWS Config, use the `subscribe` with the following parameters:

The `subscribe` command uses the following options:

`--s3-bucket`

Specify the name of an Amazon S3 bucket existing in your account or existing in another account.

`--sns-topic`

Specify the Amazon Resource Name (ARN) of an SNS topic existing in your account or existing in another account.

`--iam-role`

Specify the Amazon Resource Name (ARN) of an existing IAM Role.

The specified IAM role must have policies attached that grant AWS Config permissions to deliver configuration items to the Amazon S3 bucket and the Amazon SNS topic, and the role must grant permissions to the `Describe` APIs of the supported AWS resources.

Your command should look like the following example:

```
$ aws configservice subscribe --s3-bucket my-config-bucket --sns-topic arn:aws:sns:us-east-2:012345678912:my-config-notice --iam-role arn:aws:iam::012345678912:role/myConfigRole
```

After you run the `subscribe` command, AWS Config records all supported resources that it finds in the region. If you don't want AWS Config to record supported resources, specify the types of resources to record by updating the configuration recorder to use a recording group. For more information, see [Selecting Resources \(AWS CLI\)](#) (p. 63).

## Verify that AWS Config Is On

Once you have turned on AWS Config, you can use AWS CLI commands to verify that the AWS Config is running and that the `subscribe` command has created a configuration recorder and a delivery channel. You can also confirm that AWS Config has started recording and delivering configurations to the delivery channel.

### Contents

- [Verify that the Delivery Channel Is Created](#) (p. 31)
- [Verify that the Configuration Recorder Is Created](#) (p. 32)
- [Verify that AWS Config has started recording](#) (p. 32)

## Verify that the Delivery Channel Is Created

Use the `describe-delivery-channels` command to verify that your Amazon S3 bucket and Amazon SNS topic is configured.

```
$ aws configservice describe-delivery-channels
```

```
{
  "DeliveryChannels": [
    {
      "snsTopicARN": "arn:aws:sns:us-west-2:0123456789012:my-config-topic",
      "name": "my-delivery-channel",
      "s3BucketName": "my-config-bucket"
    }
  ]
}
```

When you use the CLI, the service API, or the SDKs to configure your delivery channel and do not specify a name, AWS Config automatically assigns the name "default".

## Verify that the Configuration Recorder Is Created

Use the `describe-configuration-recorders` command to verify that a configuration recorder is created and that the configuration recorder has assumed an IAM role. For more information, see [Creating an IAM Role \(p. 29\)](#).

```
$ aws configservice describe-configuration-recorders
{
  "ConfigurationRecorders": [
    {
      "roleARN": "arn:aws:iam::012345678912:role/myConfigRole",
      "name": "default"
    }
  ]
}
```

## Verify that AWS Config has started recording

Use the `describe-configuration-recorder-status` command to verify that the AWS Config has started recording the configurations of the supported AWS resources existing in your account. The recorded configurations are delivered to the specified delivery channel.

```
$ aws configservice describe-configuration-recorder-status
{
  "ConfigurationRecordersStatus": [
    {
      "name": "default",
      "lastStatus": "SUCCESS",
      "lastStopTime": 1414511624.914,
      "lastStartTime": 1414708460.276,
      "recording": true,
      "lastStatusChangeTime": 1414816537.148,
      "lastErrorMessage": "NA",
      "lastErrorCode": "400"
    }
  ]
}
```

The value `true` in the `recording` field confirms that the configuration recorder has started recording configurations of all your resources. AWS Config records the time in UTC. The output is displayed as a Unix timestamp.

For information about looking up the resources existing in your account and understanding the configurations of your resources, see [View, and Manage Your AWS Resources \(p. 43\)](#).

## Setting Up AWS Config Rules with the Console

The **Rules** page provides initial AWS managed rules that you can add to your account. After set up, AWS Config evaluates your AWS resources against the rules that you choose. You can update the rules and create additional managed rules after set up.

To see the complete list of AWS managed rules, see [List of AWS Config Managed Rules \(p. 103\)](#).

For example, you can choose the **cloudtrail-enabled** rule, which evaluates whether your account has a CloudTrail trail. If your account doesn't have a trail, AWS Config flags the resource type and the rule as noncompliant.

On the **Rules** page, you can do the following:

- Type in the search field to filter results by rule name, description, or label. For example, type **EC2** to return rules that evaluate EC2 resource types or type **periodic** to return rules that have a periodic trigger. Type "new" to search for newly added rules. For more information about trigger types, see [Specifying Triggers for AWS Config Rules \(p. 101\)](#).
- Choose a rule to view its specific details. You can also reorder the results alphabetically by choosing the arrow by the **Rule name** label.
- Choose the arrow icon to see the next page of rules.
- See recently added rules that are marked as **New**.
- See labels to identify the resource type that a rule evaluates and if the rule has a periodic trigger.

### To set up AWS Config rules

1. On the **Rules** page, choose the rules that you want. You can customize these rules and add other rules to your account after set up.
2. Choose **Next**.
3. On the **Review** page, verify your setup details, and then choose **Confirm**.

The **Rules** page shows your rules and their current compliance results in the table. The result for each rule is **Evaluating...** until AWS Config finishes evaluating your resources against the rule. You can update the results with the refresh button. When AWS Config finishes evaluations, you can see the rules and resource types that are compliant or noncompliant. For more information, see [Viewing Configuration Compliance \(p. 98\)](#).

#### Note

AWS Config evaluates only the resource types that it is recording. For example, if you add the **cloudtrail-enabled** rule but don't record the CloudTrail trail resource type, AWS Config can't evaluate whether the trails in your account are compliant or noncompliant. For more information, see [Selecting Which Resources AWS Config Records \(p. 62\)](#).

You can view, edit, and delete your existing rules. You can also create additional AWS managed rules or create your own. For more information, see [Managing your AWS Config Rules \(p. 207\)](#).

## Viewing the AWS Config Dashboard

Use the **Dashboard** to see an overview of your resources, rules, and their compliance state. This page helps you quickly identify the top resources in your account, and if you have any rules or resources that are noncompliant.

After setup, AWS Config starts recording the specified resources and then evaluates them against your rules. It may take a few minutes for AWS Config to display your resources, rules, and their compliance states on the **Dashboard**.

### To use the AWS Config Dashboard

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. Choose **Dashboard**.
3. Use the **Dashboard** to see an overview of your resources, rules, and their compliance state. You can do the following:
  - View the total number of resources that AWS Config is recording.
  - View the resource types that AWS Config is recording, in descending order (the number of resources). Choose a resource type to go to the **Resources inventory** page.
  - View the number of noncompliant rules.
  - View the number of noncompliant resources.
  - View the top noncompliant rules, in descending order (the number of resources).
  - Choose **View all noncompliant rules** to go to the **Rules** page.

The **Dashboard** shows the resources and rules specific to your region and account. It does not show resources or rules from other regions or other AWS accounts.

#### Note

The **Evaluate your AWS resource configuration using Config rules** message can appear on the **Dashboard** for the following reasons:

- You haven't set up AWS Config Rules for your account. You can choose **Add rule** to go to the **Rules** page.
- AWS Config is still evaluating your resources against your rules. You can refresh the page to see the latest evaluation results.
- AWS Config evaluated your resources against your rules and did not find any resources in scope. You can specify the resources for AWS Config to record in the **Settings** page. For more information, see [Selecting Which Resources AWS Config Records \(p. 62\)](#).

# Viewing AWS Resource Configurations and Managing AWS Config

Use AWS Config for the following:

- View all the resources that AWS Config is recording in your account.
- Customize the types of resources that AWS Config records.
- View configuration changes over a specific period of time for a resource in AWS Config console and AWS CLI.
- View AWS resource configuration history
- View AWS resource compliance history
- View all the notifications that AWS Config sends to an Amazon SNS topic.
- Modify settings for your IAM role
- Modify or delete your delivery channels

## Topics

- [Region Support \(p. 35\)](#)
- [Components of a Configuration Item \(p. 37\)](#)
- [Record Configurations for Third-Party Resources \(p. 38\)](#)
- [Viewing AWS Resource Configurations and History \(p. 43\)](#)
- [Managing AWS Config \(p. 56\)](#)
- [Notifications that AWS Config Sends to an Amazon SNS topic \(p. 82\)](#)

## Region Support

Currently, AWS Config is supported in the following regions:

Region Name	Region	Endpoint	Protocol
Africa (Cape Town)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Middle East (Bahrain)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Asia Pacific (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asia Pacific (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia Pacific (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS

Region Name	Region	Endpoint	Protocol
Asia Pacific (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asia Pacific (Singapore)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pacific (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
AWS GovCloud (US-East)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (US-West)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS
Canada (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Europe (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europe (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europe (Ireland)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europe (London)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europe (Milan)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europe (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
South America (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
US West (N. California)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS

## Components of a Configuration Item

A configuration item consists of the following components.

Component	Description	Contains
Metadata	Information about this configuration item	<ul style="list-style-type: none"> <li>Version ID</li> <li>Time when the configuration item was captured</li> <li>Status of the configuration item indicating whether the item was captured successfully</li> <li>State ID indicating the ordering of the configuration items of a resource</li> </ul>
Attributes <sup>1</sup>	Resource attributes	<ul style="list-style-type: none"> <li>Resource ID</li> <li>List of key–value tags<sup>2</sup> for this resource</li> <li>Resource type; see <a href="#">Supported Resource Types (p. 9)</a></li> <li>Amazon Resource Name (ARN)</li> <li>Availability Zone that contains this resource, if applicable</li> <li>Time the resource was created</li> </ul>
Relationships	How the resource is related to other resources associated with the account	Description of the relationship, such as Amazon EBS volume <code>vol-1234567</code> is attached to an Amazon EC2 instance <code>i-a1b2c3d4</code>
Current configuration	Information returned through a call to the Describe or List API of the resource	<p>For example, <code>DescribeVolumes</code> API returns the following information about the volume:</p> <ul style="list-style-type: none"> <li>Availability Zone the volume is in</li> <li>Time the volume was attached</li> <li>ID of the EC2 instance it is attached to</li> <li>Current status of the volume</li> <li>State of <code>DeleteOnTermination</code> flag</li> <li>Device the volume is attached to</li> <li>Type of volume, such as <code>gp2</code>, <code>io1</code>, or <code>standard</code></li> </ul>

### Notes

1. A configuration item relationship does not include network flow or data flow dependencies. Configuration items cannot be customized to represent your application architecture.
2. AWS Config does not record key–value tags for CloudTrail trail, CloudFront distribution, and CloudFront streaming distribution.
3. As of Version 1.3, the `relatedEvents` field is empty. You can access the [LookupEvents API](#) in the *AWS CloudTrail API Reference* to retrieve the events for the resource.
4. As of Version 1.3, the `configurationItemMD5Hash` field is empty. You can use the `configurationStateId` field to ensure you have the latest configuration item.

# Record Configurations for Third-Party Resources

Record configurations for third-party resources or custom resource types such as on premise servers, SAAS monitoring tools, and version control systems (like GitHub). You can publish the configuration data of third-party resources into AWS Config and view and monitor the resource inventory and configuration history using AWS Config console and APIs. Now, you can use AWS Config to manage all your resources and evaluate resource configuration for compliance against best practices using AWS Config rules. You can also create AWS Config rules or conformance packs to evaluate these third-party resources against best practices, internal policies, and regulatory policies.

## Note

This feature is only available in the redesigned AWS Config console.

If you have configured AWS Config to record all resource types, then third-party resources that are managed (i.e. created/updated/deleted) through AWS CloudFormation are automatically tracked in AWS Config as configuration items.

**Prerequisite:** The third-party resources or custom resource type must be registered using AWS CloudFormation.

## Topics

- [Step 1: Setup Your Development Environment \(p. 38\)](#)
- [Step 2: Model Your Resource \(p. 38\)](#)
- [Step 3: Generate Artifacts \(p. 40\)](#)
- [Step 4: Register Your Resource \(p. 40\)](#)
- [Step 5: Publish Resource Configuration \(p. 40\)](#)
- [Record and Delete a Configuration State for Third-Party Resources Using AWS CLI \(p. 40\)](#)
- [Managing a Configuration State for Third-Party Resources Type Using APIs \(p. 42\)](#)
- [Region Support \(p. 42\)](#)

## Step 1: Setup Your Development Environment

Install and configure AWS CloudFormation AWS CLI. The AWS CLI allows you to model and register your custom resources. For more information, see [Custom Resources](#) and [What Is the CloudFormation Command Line Interface?](#).

## Step 2: Model Your Resource

Create a resource provider schema that conforms to and validates the configuration of the resource type.

1. Use the `init` command to create your resource provider project and generate the files it requires.

```
$ cfn init
Initializing new project
```

2. The `init` command launches a wizard that walks you through setting up the project, including specifying the resource name. For this walkthrough, specify `MyCustomNamespace::Testing::WordPress`.

```
Enter resource type identifier (Organization::Service::Resource):
MyCustomNamespace::Testing::WordPress
```

3. Enter a package name for your resource.

```
Enter a package name (empty for default 'com.custom.testing.wordpress'):  
com.custom.testing.wordpress  
Initialized a new project in /workplace/user/custom-testing-wordpress
```

### Note

In order to guarantee that any project dependencies are correctly resolved, you can import the generated project into your IDE with Maven support.

For example, if you are using IntelliJ IDEA, you would need to do the following:

- From the **File** menu, choose **New**, then choose **Project From Existing Sources**.
  - Navigate to the project directory
  - In the **Import Project** dialog box, choose **Import project from external model** and then choose **Maven**.
  - Choose **Next** and accept any defaults to complete importing the project.
4. Open the `mycustomnamespace-testing-wordpress.json` file that contains the schema for your resource. Copy and paste the following schema into `mycustomnamespace-testing-wordpress.json`.

```
{  
  "typeName": "MyCustomNamespace::Testing::WordPress",  
  "description": "An example resource that creates a website based on WordPress  
5.2.2.",  
  "properties": {  
    "Name": {  
      "description": "A name associated with the website.",  
      "type": "string",  
      "pattern": "^[a-zA-Z0-9]{1,219}\\Z",  
      "minLength": 1, "maxLength": 219  
    },  
    "SubnetId": {  
      "description": "A subnet in which to host the website.",  
      "pattern": "^(subnet-[a-f0-9]{13})|(subnet-[a-f0-9]{8})\\Z",  
      "type": "string"  
    },  
    "InstanceId": {  
      "description": "The ID of the instance that backs the WordPress site.",  
      "type": "string"  
    },  
    "PublicIp": {  
      "description": "The public IP for the WordPress site.",  
      "type": "string"  
    }  
  },  
  "required": [ "Name", "SubnetId" ],  
  "primaryIdentifier": [ "/properties/PublicIp", "/properties/InstanceId" ],  
  "readOnlyProperties": [ "/properties/PublicIp", "/properties/InstanceId" ],  
  "additionalProperties": false  
}
```

5. Validate the schema.

```
$ cfn validate
```

6. Update the auto-generated files in the resource provider package to view the resource provider schema updates. Upon initiation of the resource provider project, the AWS CLI generates supporting files and code for the resource provider. Regenerate the code to see the updated schema.

```
$ cfn generate
```

**Note**

When using Maven, as part of the build process the `generate` command is automatically run before the code is compiled. So your changes will never get out of sync with the generated code.

Be aware the CloudFormation CLI must be in a location Maven/the system can find. For more information, see [Setting up your environment for developing extensions](#).

For more information on the whole process, see [Modeling Resource Providers for Use in AWS CloudFormation](#).

## Step 3: Generate Artifacts

Run the following command to generate artifacts for `cfn submit`.

```
$ mvn package
```

## Step 4: Register Your Resource

AWS Config does not require resource provider handlers to perform configuration tracking for your resource. Run the following command to register your resource.

```
$ cfn submit
```

For more information, see [Registering Resource Providers for Use in AWS CloudFormation Templates](#).

## Step 5: Publish Resource Configuration

Determine the configuration for `MyCustomNamespace::Testing::WordPress`.

```
{
  "Name": "MyWordPressSite",
  "SubnetId": "subnet-abcd0123",
  "InstanceId": "i-01234567",
  "PublicIp": "my-wordpress-site.com"
}
```

Determine the schema version id from AWS CloudFormation `DescribeType`.

In the AWS Config see if this resource configuration is accepted. To evaluate compliance you can write AWS Config rules using this resource. For additional information, see [Record and Delete a Configuration State for Third-Party Resources Using AWS CLI](#).

Optional: To automate recording of configuration, implement a periodic or change-based configuration collectors.

## Record and Delete a Configuration State for Third-Party Resources Using AWS CLI

The AWS CLI is a unified tool to manage your AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and use scripts to automate them.

To install the AWS CLI on your local machine, see [Installing the AWS CLI](#) in the *AWS CLI User Guide*.

If necessary, type `aws configure` to configure the AWS CLI.

### Topics

- [Record a Configuration Item \(p. 41\)](#)
- [Read the Configuration Item using AWS Config APIs \(p. 41\)](#)
- [Delete the Third-Party Resource \(p. 42\)](#)

## Record a Configuration Item

Record a configuration item for a third-party resource or a custom resource type using the following procedure:

Ensure you register the resource type `MyCustomNamespace::Testing::WordPress` with its matching schema.

1. Open a command prompt or a terminal window.
2. Type the following command:

```
aws configservice put-resource-config --resource-type
MyCustomNamespace::Testing::WordPress --resource-id resource-001 --schema-version-id
00000001 --configuration '{
  "Id": "resource-001",
  "Name": "My example custom resource.",
  "PublicAccess": false
}'
```

### Note

As defined in the type schema, `writeOnlyProperties` will be removed from the configuration prior to being recorded by AWS Config. This means that these values will not be present when the configuration is obtained via read APIs. For more information on `writeOnlyProperties`, see [Resource type schema](#).

## Read the Configuration Item using AWS Config APIs

1. Open a command prompt or a terminal window.
2. Type the following command:

```
aws configservice list-discovered-resources --resource-type
MyCustomNamespace::Testing::WordPress
```

3. Press Enter.

You should see output similar to the following:

```
{
  "resourceIdentifiers": [
    {
      "resourceType": "MyCustomNamespace::Testing::WordPress",
      "resourceId": "resource-001"
    }
  ]
}
```

4. Type the following command:

```
aws configservice batch-get-resource-config --resource-keys '[ { "resourceType":  
  "MyCustomNamespace::Testing::WordPress", "resourceId": "resource-001" } ]'
```

5. Press Enter.

You should see output similar to the following:

```
{  
  "unprocessedResourceKeys": [],  
  "baseConfigurationItems": [  
    {  
      "configurationItemCaptureTime": 1569605832.673,  
      "resourceType": "MyCustomNamespace::Testing::WordPress",  
      "resourceId": "resource-001",  
      "configurationStateId": "1569605832673",  
      "awsRegion": "us-west-2",  
      "version": "1.3",  
      "supplementaryConfiguration": {},  
      "configuration": "{\\"Id\\":\\"resource-001\\",\\"Name\\":\\"My example custom  
resource.\",\\"PublicAccess\\":false}",  
      "configurationItemStatus": "ResourceDiscovered",  
      "accountId": "AccountId"  
    }  
  ]  
}
```

## Delete the Third-Party Resource

You can record the configuration state for a third-party resource or custom resource type that you want to delete.

- Type the following command:

```
aws configservice delete-resource-config --resource-type  
  MyCustomNamespace::Testing::WordPress --resource-id resource-002
```

If successful, the command executes with no additional output.

## Managing a Configuration State for Third-Party Resources Type Using APIs

You can manage a configuration state for third-party resources or custom resource type using **PutResourceConfig** and **DeleteResourceConfig** APIs. For more information, see the API Reference.

- [PutResourceConfig](#)
- [DeleteResourceConfig](#)

## Region Support

This feature is supported in the following regions:

Region Name	Region	Endpoint	Protocol
Asia Pacific (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia Pacific (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asia Pacific (Singapore)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pacific (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canada (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Europe (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europe (Ireland)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europe (London)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europe (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europe (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
South America (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
US West (N. California)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS

## Viewing AWS Resource Configurations and History

You can view all of the resources that AWS Config is recording in your account, the configuration changes that took place for a resource over a specified time period, and the relationships of the selected resource with all the related resources. You can also view compliance state changes for resources as evaluated by AWS Config Rules displayed in a timeline.

### Topics

- [Looking Up Resources That Are Discovered by AWS Config \(p. 44\)](#)
- [Viewing Configuration Details \(p. 45\)](#)
- [Viewing Compliance History Timeline for Resources \(p. 49\)](#)
- [Delivering Configuration Snapshot to an Amazon S3 Bucket \(p. 51\)](#)

## Looking Up Resources That Are Discovered by AWS Config

You can use the AWS Config console, AWS CLI, and AWS Config API to look up the resources that AWS Config has taken an inventory of, or *discovered*, including deleted resources and resources that AWS Config is not currently recording. AWS Config discovers supported resource types only. For more information, see [Supported Resource Types \(p. 9\)](#).

### Looking Up Resources (AWS Config Console)

You can use resource types or tag information to look up resources in the AWS Config console.

#### To look up resources

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. On the **Resource inventory** page, specify the search options for the resources that you want to look up:
  - Choose **Resources** and then choose one or more resource types in the list. This list includes resource types that AWS Config supports. To narrow results, type a resource ID or, if applicable, a resource name in the next box. You can also choose **Include deleted resources**.
  - Choose **Tag** and type a tag key that is applied to your resources, such as **CostCenter**. To narrow results, type a tag value in the next box.
3. After you specify the search options, choose **Look up**.
4. AWS Config lists the resources that match your search options. You can see the following information about the resources:
  - **Resource identifier** – The resource identifier might be a resource ID or a resource name, if applicable. Choose the resource identifier link to view the resource details page.
  - **Resource type** – The type of the resource is listed.
  - **Compliance** – The status of the resource that AWS Config evaluated against your rule.

For more information, see [Viewing Configuration Details \(p. 45\)](#).

### Looking Up Resources (AWS CLI)

You can use the AWS CLI to list resources that AWS Config has discovered.

#### To look up resources (AWS CLI)

- Use the `aws configservice list-discovered-resources` command:

#### Example

```
$ aws configservice list-discovered-resources --resource-type "AWS::EC2::Instance"
```

```
{
  "resourceIdentifiers": [
    {
      "resourceType": "AWS::EC2::Instance",
      "resourceId": "i-nnnnnnnn"
    }
  ]
}
```

To view the configuration details of a resource that is listed in the response, use the `get-resource-config-history` command, and specify the resource type and ID. For an example of this command and the response from AWS Config, see [Viewing Configuration History \(p. 45\)](#).

## Looking up Resources (AWS Config API)

You specify a resource type, and AWS Config returns a list of resource identifiers for resources of that type. For more information, see [ResourceIdentifier](#) in the *AWS Config API Reference*.

### To look up resources (AWS Config API)

- Use the [ListDiscoveredResources](#) action.

To get the configuration details of a resource that is listed in the response, use the [GetResourceConfigHistory](#) action, and specify the resource type and ID.

## Viewing Configuration Details

You can view the configuration, relationships, and number of changes made to a resource in the AWS Config console. You can view the configuration history for a resource using AWS CLI.

### Viewing Configuration Details (Console)

When you look up resources on the **Resource inventory** page, choose the resource name or ID in the resource identifier column to view the resource's details page. The details page provides information about the configuration, relationships, and number of changes made to that resource.

To access the resource timeline from the resource details page, choose the **Resource Timeline** button.

### Viewing Configuration Details (AWS CLI)

The configuration items that AWS Config records are delivered to the specified delivery channel on demand as a configuration snapshot and as a configuration stream. You can use the AWS CLI to view history of configuration items for each resource.

### Viewing Configuration History

Type the `get-resource-config-history` command and specify the resource type and the resource ID, for example:

```
$ aws configservice get-resource-config-history --resource-type AWS::EC2::SecurityGroup --
resource-id sg-6fbb3807
{
  "configurationItems": [
    {
      "configurationItemCaptureTime": 1414708529.9219999,
      "relationships": [
        {
```

```

        "resourceType": "AWS::EC2::Instance",
        "resourceId": "i-7a3b232a",
        "relationshipName": "Is associated with Instance"
    },
    {
        "resourceType": "AWS::EC2::Instance",
        "resourceId": "i-8b6eb2ab",
        "relationshipName": "Is associated with Instance"
    },
    {
        "resourceType": "AWS::EC2::Instance",
        "resourceId": "i-c478efe5",
        "relationshipName": "Is associated with Instance"
    },
    {
        "resourceType": "AWS::EC2::Instance",
        "resourceId": "i-e4cbe38d",
        "relationshipName": "Is associated with Instance"
    }
},
"availabilityZone": "Not Applicable",
"tags": {},
"resourceType": "AWS::EC2::SecurityGroup",
"resourceId": "sg-6fbb3807",
"configurationStateId": "1",
"relatedEvents": [],
"arn": "arn:aws:ec2:us-east-2:012345678912:security-group/default",
"version": "1.0",
"configurationItemMD5Hash": "860aa81fc3869e186b2ee00bc638a01a",
"configuration": "{\"ownerId\": \"605053316265\", \"groupName\": \"default
\\\", \"groupId\": \"sg-6fbb3807\", \"description\": \"default group\", \"ipPermissions\":
[ { \"ipProtocol\": \"tcp\", \"fromPort\": 80, \"toPort\": 80, \"userIdGroupPairs\": [ { \"userId
\\\": \"amazon-elb\", \"groupName\": \"amazon-elb-sg\", \"groupId\": \"sg-843f59ed\" } ] },
\\\"ipRanges\": [ \"0.0.0.0/0\" ] }, { \"ipProtocol\": \"tcp\", \"fromPort\": 0, \"toPort\": 65535,
\\\"userIdGroupPairs\": [ { \"userId\": \"605053316265\", \"groupName\": \"default\", \"groupId
\\\": \"sg-6fbb3807\" } ] }, { \"ipProtocol\": \"udp\", \"fromPort\": 0, \"toPort
\\\": 65535, \"userIdGroupPairs\": [ { \"userId\": \"605053316265\", \"groupName\": \"default\",
\\\"groupId\": \"sg-6fbb3807\" } ] }, { \"ipProtocol\": \"icmp\", \"fromPort\": -1,
\\\"toPort\": -1, \"userIdGroupPairs\": [ { \"userId\": \"605053316265\", \"groupName\": \"default
\\\", \"groupId\": \"sg-6fbb3807\" } ] }, { \"ipProtocol\": \"tcp\", \"fromPort
\\\": 1433, \"toPort\": 1433, \"userIdGroupPairs\": [ ], \"ipRanges\": [ \"0.0.0.0/0\" ] }, { \"ipProtocol
\\\": \"tcp\", \"fromPort\": 3389, \"toPort\": 3389, \"userIdGroupPairs\": [ ], \"ipRanges\":
[ \"207.171.160.0/19\" ] }, \"ipPermissionsEgress\": [ ], \"vpcId\": null, \"tags\": [ ] }\",
    "configurationItemStatus": "ResourceDiscovered",
    "accountId": "605053316265"
}
},
"nextToken":
.....

```

For detailed explanation of the response fields, see [Components of a Configuration Item \(p. 37\)](#) and [Supported Resource Types \(p. 9\)](#).

## Example Amazon EBS Configuration History from AWS Config

AWS Config generates a set of files that each represent a resource type and lists all configuration changes for the resources of that type that AWS Config is recording. AWS Config exports this resource-centric configuration history as an object in the Amazon S3 bucket that you specified when you enabled AWS Config. The configuration history file for each resource type contains the changes that were detected for the resources of that type since the last history file was delivered. The history files are typically delivered every six hours.

The following is an example of the contents of the Amazon S3 object that describes the configuration history of all the Amazon Elastic Block Store volumes in the current region for your AWS account. The

volumes in this account include `vol-ce676ccc` and `vol-cia007c`. Volume `vol-ce676ccc` had two configuration changes since the previous history file was delivered while volume `vol-cia007c` had one change.

```
{
  "fileVersion": "1.0",
  "requestId": "asudf8ow-4e34-4f32-afeb-0ace5bf3trye",
  "configurationItems": [
    {
      "snapshotVersion": "1.0",
      "resourceId": "vol-ce676ccc",
      "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
      "accountId": "12345678910",
      "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
      "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
      "configurationItemStatus": "OK",
      "relatedEvents": [
        "06c12a39-eb35-11de-ae07-adb69edbb1e4",
        "c376e30d-71a2-4694-89b7-a5a04ad92281"
      ],
      "availabilityZone": "us-west-2b",
      "resourceType": "AWS::EC2::Volume",
      "resourceCreationTime": "2014-02-27T21:43:53.885Z",
      "tags": {},
      "relationships": [
        {
          "resourceId": "i-344c463d",
          "resourceType": "AWS::EC2::Instance",
          "name": "Attached to Instance"
        }
      ],
      "configuration": {
        "volumeId": "vol-ce676ccc",
        "size": 1,
        "snapshotId": "",
        "availabilityZone": "us-west-2b",
        "state": "in-use",
        "createTime": "2014-02-27T21:43:53.0885+0000",
        "attachments": [
          {
            "volumeId": "vol-ce676ccc",
            "instanceId": "i-344c463d",
            "device": "/dev/sdf",
            "state": "attached",
            "attachTime": "2014-03-07T23:46:28.0000+0000",
            "deleteOnTermination": false
          }
        ],
        "tags": [
          {
            "tagName": "environment",
            "tagValue": "PROD"
          },
          {
            "tagName": "name",
            "tagValue": "DataVolume1"
          }
        ],
        "volumeType": "standard"
      }
    },
    {
      "configurationItemVersion": "1.0",
      "resourceId": "vol-ce676ccc",
      "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",

```

```

"accountId": "12345678910",
"configurationItemCaptureTime": "2014-03-07T21:47:08.918Z",
"configurationItemState": "3e660fdf-4e34-4f32-sseb-0ace5bf3d63a",
"configurationItemStatus": "OK",
"relatedEvents": [
  "06c12a39-eb35-11de-ae07-ad229edbb1e4",
  "c376e30d-71a2-4694-89b7-a5a04w292281"
],
"availabilityZone": "us-west-2b",
"resourceType": "AWS::EC2::Volume",
"resourceCreationTime": "2014-02-27T21:43:53.885Z",
"tags": {},
"relationships": [
  {
    "resourceId": "i-344c463d",
    "resourceType": "AWS::EC2::Instance",
    "name": "Attached to Instance"
  }
],
"configuration": {
  "volumeId": "vol-ce676ccc",
  "size": 1,
  "snapshotId": "",
  "availabilityZone": "us-west-2b",
  "state": "in-use",
  "createTime": "2014-02-27T21:43:53.0885+0000",
  "attachments": [
    {
      "volumeId": "vol-ce676ccc",
      "instanceId": "i-344c463d",
      "device": "/dev/sdf",
      "state": "attached",
      "attachTime": "2014-03-07T23:46:28.0000+0000",
      "deleteOnTermination": false
    }
  ],
  "tags": [
    {
      "tagName": "environment",
      "tagValue": "PROD"
    },
    {
      "tagName": "name",
      "tagValue": "DataVolume1"
    }
  ],
  "volumeType": "standard"
}
},
{
  "configurationItemVersion": "1.0",
  "resourceId": "vol-cia007c",
  "arn": "arn:aws:us-west-2b:123456789012:volume/vol-cia007c",
  "accountId": "12345678910",
  "configurationItemCaptureTime": "2014-03-07T20:47:08.918Z",
  "configurationItemState": "3e660fdf-4e34-4f88-sseb-0ace5bf3d63a",
  "configurationItemStatus": "OK",
  "relatedEvents": [
    "06c12a39-eb35-11de-ae07-adjhk8edbb1e4",
    "c376e30d-71a2-4694-89b7-a5a67u292281"
  ],
  "availabilityZone": "us-west-2b",
  "resourceType": "AWS::EC2::Volume",
  "resourceCreationTime": "2014-02-27T20:43:53.885Z",
  "tags": {},
  "relationships": [

```

```
    {
      "resourceId": "i-344e563d",
      "resourceType": "AWS::EC2::Instance",
      "name": "Attached to Instance"
    }
  ],
  "configuration": {
    "volumeId": "vol-cia007c",
    "size": 1,
    "snapshotId": "",
    "availabilityZone": "us-west-2b",
    "state": "in-use",
    "createTime": "2014-02-27T20:43:53.0885+0000",
    "attachments": [
      {
        "volumeId": "vol-cia007c",
        "instanceId": "i-344e563d",
        "device": "/dev/sdf",
        "state": "attached",
        "attachTime": "2014-03-07T23:46:28.0000+0000",
        "deleteOnTermination": false
      }
    ],
    "tags": [
      {
        "tagName": "environment",
        "tagValue": "PROD"
      },
      {
        "tagName": "name",
        "tagValue": "DataVolume2"
      }
    ],
    "volumeType": "standard"
  }
}
]
```

## Viewing Compliance History Timeline for Resources

AWS Config supports storing compliance state changes of resources as evaluated by AWS Config Rules. The resource compliance history is presented in the form of a timeline. The timeline captures changes as `ConfigurationItems` over a period of time for a specific resource. The resource timeline is available in the AWS Config console adjacent to the Configuration timeline.

You can opt in or out to record all resource types in AWS Config. If you have opted to record all resource types, AWS Config automatically begins to recording the resource compliance history as evaluated by AWS Config Rules. By default, AWS Config records the configuration changes for all supported resources. You can also select only the specific resource compliance history resource type: `AWS::Config::ResourceCompliance`. For more information, see [Selecting Which Resources AWS Config Records](#).

## Viewing Resource Timeline Using Resources

Access the resource timeline by selecting a specific resource from the Resource inventory page.

1. Select the **Resources** from the left navigation.
2. On the Resource inventory page, select all the existing resources from the drop-down and if appropriate, select include deleted resources.

The table displays the resource identifier for the resource type and the resource compliance status for that resource. The resource identifier might be a resource ID or a resource name, if applicable.

3. Select the resource from the resource identifier column.
4. Select the **Resource Timeline** button.

**Note**

Alternatively, on the Resource inventory page, you can directly choose the resource name. To access the resource timeline from the resource details page, choose the **Resource Timeline** button.

## Viewing Resource Timeline Using Rules

Access the resource timeline by selecting a specific rule from the Rule page.

1. Select the **Rules** from the left navigation.
2. On the Rule page, choose a rule evaluating your relevant resources. If no rules are displayed on the screen, add rules using the **Add rule** button.
3. On the Rule details page, select the resources from the Resources evaluated table.
4. Select the **Resource Timeline** button. The resource timeline is displayed.

## Querying Compliance History

Query the resource compliance history using `get-resource-config-history` using the resource type `AWS::Config::ResourceCompliance`.

```
aws configservice get-resource-config-history --resource-type  
AWS::Config::ResourceCompliance --resource-id AWS::S3::Bucket/configrules-bucket
```

You should see output similar to the following:

```
{  
  "configurationItems": [  
    {  
      "configurationItemCaptureTime": 1539799966.921,  
      "relationships": [  
        {  
          "resourceType": "AWS::S3::Bucket",  
          "resourceId": "configrules-bucket",  
          "relationshipName": "Is associated with "  
        }  
      ]  
    },  
    {  
      "tags": {},  
      "resourceType": "AWS::Config::ResourceCompliance",  
      "resourceId": "AWS::S3::Bucket/configrules-bucket",  
      "ConfigurationStateId": "1539799966921",  
      "relatedEvents": [];  
      "awsRegion": "us-west-2",  
      "version": "1.3",  
      "configurationItemMD5Hash": "",  
      "supplementaryConfiguration": {},  
      "configuration": "{\"complianceType\":\"COMPLIANT\", \"targetResourceId\":\"configrules-  
bucket\", \"targetResourceType\":\"AWS::S3::Bucket\", \"configRuleList\":[{\"configRuleArn  
\": \"arn:aws:config:us-west-2:AccountID:config-rule/config-rule-wlgogw\", \"configRuleId\":  
\"config-rule-wlgogw\", \"configRuleName\":\"s3-bucket-logging-enabled\", \"complianceType\":  
\"COMPLIANT\"}]}",
```

```
"configurationItemStatus": "ResourceDiscovered",  
"accountId": "AccountID"  
}  
]  
}
```

## Delivering Configuration Snapshot to an Amazon S3 Bucket

AWS Config delivers configuration items of the AWS resources that AWS Config is recording to the Amazon S3 bucket that you specified when you configured your delivery channel.

### Topics

- [Delivering Configuration Snapshot \(p. 51\)](#)
- [Example Configuration Snapshot from AWS Config \(p. 51\)](#)
- [Verifying Delivery Status \(p. 55\)](#)
- [Viewing Configuration Snapshot in Amazon S3 bucket \(p. 55\)](#)

## Delivering Configuration Snapshot

AWS Config generates configuration snapshots when you invoke the [DeliverConfigSnapshot](#) action or you run the AWS CLI `deliver-config-snapshot` command. AWS Config stores configuration snapshots in the Amazon S3 bucket that you specified when you enabled AWS Config.

Type the `deliver-config-snapshot` command by specifying the name assigned by AWS Config when you configured your delivery channel, for example:

```
$ aws configservice deliver-config-snapshot --delivery-channel-name default  
{  
  "configSnapshotId": "94ccff53-83be-42d9-996f-b4624b3c1a55"  
}
```

## Example Configuration Snapshot from AWS Config

The following is an example of the information that AWS Config includes in a configuration snapshot. The snapshot describes the configuration for the resources that AWS Config is recording in the current region for your AWS account, and it describes the relationships between these resources.

### Note

The configuration snapshot can include references to resources types and resource IDs that are not supported.

```
{  
  "fileVersion": "1.0",  
  "requestId": "asudf8ow-4e34-4f32-afeb-0ace5bf3trye",  
  "configurationItems": [  
    {  
      "configurationItemVersion": "1.0",  
      "resourceId": "vol-ce676ccc",  
      "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",  
      "accountId": "12345678910",  
      "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",  
      "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",  
    }  
  ]  
}
```

```
"configurationItemStatus": "OK",
"relatedEvents": [
  "06c12a39-eb35-11de-ae07-adb69edbb1e4",
  "c376e30d-71a2-4694-89b7-a5a04ad92281"
],
"availabilityZone": "us-west-2b",
"resourceType": "AWS::EC2::Volume",
"resourceCreationTime": "2014-02-27T21:43:53.885Z",
"tags": {},
"relationships": [
  {
    "resourceId": "i-344c463d",
    "resourceType": "AWS::EC2::Instance",
    "name": "Attached to Instance"
  }
],
"configuration": {
  "volumeId": "vol-ce676ccc",
  "size": 1,
  "snapshotId": "",
  "availabilityZone": "us-west-2b",
  "state": "in-use",
  "createTime": "2014-02-27T21:43:53.0885+0000",
  "attachments": [
    {
      "volumeId": "vol-ce676ccc",
      "instanceId": "i-344c463d",
      "device": "/dev/sdf",
      "state": "attached",
      "attachTime": "2014-03-07T23:46:28.0000+0000",
      "deleteOnTermination": false
    }
  ],
  "tags": [
    {
      "tagName": "environment",
      "tagValue": "PROD"
    },
    {
      "tagName": "name",
      "tagValue": "DataVolume1"
    }
  ],
  "volumeType": "standard"
}
},
{
  "configurationItemVersion": "1.0",
  "resourceId": "i-344c463d",
  "accountId": "12345678910",
  "arn": "arn:aws:ec2:us-west-2b:123456789012:instance/i-344c463d",
  "configurationItemCaptureTime": "2014-03-07T23:47:09.523Z",
  "configurationStateID": "cdb571fa-ce7a-4ec5-8914-0320466a355e",
  "configurationItemStatus": "OK",
  "relatedEvents": [
    "06c12a39-eb35-11de-ae07-adb69edbb1e4",
    "c376e30d-71a2-4694-89b7-a5a04ad92281"
  ],
  "availabilityZone": "us-west-2b",
  "resourceType": "AWS::EC2::Instance",
  "resourceCreationTime": "2014-02-26T22:56:35.000Z",
  "tags": {
    "Name": "integ-test-1",
    "examplename": "examplevalue"
  },
  "relationships": [
```

```
{
  "resourceId": "vol-ce676ccc",
  "resourceType": "AWS::EC2::Volume",
  "name": "Attached Volume"
},
{
  "resourceId": "vol-ef0e06ed",
  "resourceType": "AWS::EC2::Volume",
  "name": "Attached Volume",
  "direction": "OUT"
},
{
  "resourceId": "subnet-47b4cf2c",
  "resourceType": "AWS::EC2::SUBNET",
  "name": "Is contained in Subnet",
  "direction": "IN"
}
],
"configuration": {
  "instanceId": "i-344c463d",
  "imageId": "ami-ccf297fc",
  "state": {
    "code": 16,
    "name": "running"
  },
  "privateDnsName": "ip-172-31-21-63.us-west-2.compute.internal",
  "publicDnsName": "ec2-54-218-4-189.us-west-2.compute.amazonaws.com",
  "stateTransitionReason": "",
  "keyName": "configDemo",
  "amiLaunchIndex": 0,
  "productCodes": [],
  "instanceType": "t1.micro",
  "launchTime": "2014-02-26T22:56:35.0000+0000",
  "placement": {
    "availabilityZone": "us-west-2b",
    "groupName": "",
    "tenancy": "default"
  },
  "kernelId": "aki-fc8f11cc",
  "monitoring": {
    "state": "disabled"
  },
  "subnetId": "subnet-47b4cf2c",
  "vpcId": "vpc-41b4cf2a",
  "privateIpAddress": "172.31.21.63",
  "publicIpAddress": "54.218.4.189",
  "architecture": "x86_64",
  "rootDeviceType": "ebs",
  "rootDeviceName": "/dev/sda1",
  "blockDeviceMappings": [
    {
      "deviceName": "/dev/sda1",
      "ebs": {
        "volumeId": "vol-ef0e06ed",
        "status": "attached",
        "attachTime": "2014-02-26T22:56:38.0000+0000",
        "deleteOnTermination": true
      }
    },
    {
      "deviceName": "/dev/sdf",
      "ebs": {
        "volumeId": "vol-ce676ccc",
        "status": "attached",
        "attachTime": "2014-03-07T23:46:28.0000+0000",
        "deleteOnTermination": false
      }
    }
  ]
}
```

```
    }
  },
  "virtualizationType": "paravirtual",
  "clientToken": "aBCDe123456",
  "tags": [
    {
      "key": "Name",
      "value": "integ-test-1"
    },
    {
      "key": "examplekey",
      "value": "examplevalue"
    }
  ],
  "securityGroups": [
    {
      "groupName": "launch-wizard-2",
      "groupId": "sg-892adfec"
    }
  ],
  "sourceDestCheck": true,
  "hypervisor": "xen",
  "networkInterfaces": [
    {
      "networkInterfaceId": "eni-55c03d22",
      "subnetId": "subnet-47b4cf2c",
      "vpcId": "vpc-41b4cf2a",
      "description": "",
      "ownerId": "12345678910",
      "status": "in-use",
      "privateIpAddress": "172.31.21.63",
      "privateDnsName": "ip-172-31-21-63.us-west-2.compute.internal",
      "sourceDestCheck": true,
      "groups": [
        {
          "groupName": "launch-wizard-2",
          "groupId": "sg-892adfec"
        }
      ],
      "attachment": {
        "attachmentId": "eni-attach-bf90c489",
        "deviceIndex": 0,
        "status": "attached",
        "attachTime": "2014-02-26T22:56:35.0000+0000",
        "deleteOnTermination": true
      },
      "association": {
        "publicIp": "54.218.4.189",
        "publicDnsName": "ec2-54-218-4-189.us-
west-2.compute.amazonaws.com",
        "ipOwnerId": "amazon"
      },
      "privateIpAddresses": [
        {
          "privateIpAddress": "172.31.21.63",
          "privateDnsName": "ip-172-31-21-63.us-
west-2.compute.internal",
          "primary": true,
          "association": {
            "publicIp": "54.218.4.189",
            "publicDnsName": "ec2-54-218-4-189.us-
west-2.compute.amazonaws.com",
            "ipOwnerId": "amazon"
          }
        }
      ]
    }
  ]
}
```

```
    ]
  },
  "ebsOptimized": false
}
]
```

The next step is to verify that configuration snapshot was delivered successfully to the delivery channel.

## Verifying Delivery Status

Type the `describe-delivery-channel-status` command to verify that the AWS Config has started delivering the configurations to the specified delivery channel, for example:

```
$ aws configservice describe-delivery-channel-status
{
  "DeliveryChannelsStatus": [
    {
      "configStreamDeliveryInfo": {
        "lastStatusChangeTime": 1415138614.125,
        "lastStatus": "SUCCESS"
      },
      "configHistoryDeliveryInfo": {
        "lastSuccessfulTime": 1415148744.267,
        "lastStatus": "SUCCESS",
        "lastAttemptTime": 1415148744.267
      },
      "configSnapshotDeliveryInfo": {
        "lastSuccessfulTime": 1415333113.4159999,
        "lastStatus": "SUCCESS",
        "lastAttemptTime": 1415333113.4159999
      },
      "name": "default"
    }
  ]
}
```

The response lists the status of all the three delivery formats that AWS Config uses to deliver configurations to your bucket and topic.

Take a look at the `lastSuccessfulTime` field in `configSnapshotDeliveryInfo`. The time should match the time you last requested the delivery of the configuration snapshot.

### Note

AWS Config uses the UTC format (Coordinated Universal Time) to record the time.

## Viewing Configuration Snapshot in Amazon S3 bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the Amazon S3 console **All Buckets** list, click the name of your Amazon S3 bucket.
3. Click through the nested folders in your bucket until you see the `ConfigSnapshot` object with a snapshot ID that matches with the ID returned by the command. Download and open the object to view the configuration snapshot.

The S3 bucket also contains an empty file named `ConfigWritabilityCheckFile`. AWS Config creates this file to verify that the service can successfully write to the S3 bucket.

## Managing AWS Config

At any time, you can change the settings for your IAM role and modify or delete your delivery channel (that is, the Amazon Simple Storage Service bucket and the Amazon Simple Notification Service topic). You can start or stop the configuration recorder associated with your account, and you can customize which types of resources are recorded.

### Topics

- [Managing the Delivery Channel \(p. 56\)](#)
- [Updating the IAM Role Assigned to AWS Config \(p. 59\)](#)
- [Managing the Configuration Recorder \(p. 60\)](#)
- [Selecting Which Resources AWS Config Records \(p. 62\)](#)
- [Recording Software Configuration for Managed Instances \(p. 65\)](#)
- [Querying the Current Configuration State of AWS Resources \(p. 66\)](#)
- [Deleting AWS Config Data \(p. 80\)](#)

## Managing the Delivery Channel

As AWS Config continually records the changes that occur to your AWS resources, it sends notifications and updated configuration states through the *delivery channel*. You can manage the delivery channel to control where AWS Config sends configuration updates.

You can have only one delivery channel per region per AWS account, and the delivery channel is required to use AWS Config.

When AWS Config detects a configuration change for a resource and the notification exceeds the maximum size allowed by Amazon SNS, the notification includes a brief summary of the configuration item. You can view the complete notification in the Amazon S3 bucket location specified in the `s3BucketLocation` field. For more information, see [Example Oversized Configuration Item Change Notification](#).

### Note

AWS Config does not support the delivery channel to an Amazon S3 bucket where object lock is enabled. For more information, see [How S3 Object Lock works](#).

## Updating the Delivery Channel

When you update the delivery channel, you can set the following options:

- The Amazon S3 bucket to which AWS Config sends configuration snapshots and configuration history files.
- How often AWS Config delivers configuration snapshots to your Amazon S3 bucket.
- The Amazon SNS topic to which AWS Config sends notifications about configuration changes.

### To update the delivery channel (console)

- You can use the AWS Config console to set the Amazon S3 bucket and the Amazon SNS topic for your delivery channel. For steps to manage these settings, see [Setting Up AWS Config with the Console \(p. 25\)](#).

The console does not provide options to rename the delivery channel, set the frequency for configuration snapshots, or delete the delivery channel. To do these tasks, you must use the AWS CLI, the AWS Config API, or one of the AWS SDKs.

## To update the delivery channel (AWS CLI)

1. Use the `put-delivery-channel` command:

```
$ aws configservice put-delivery-channel --delivery-channel file://deliveryChannel.json
```

The `deliveryChannel.json` file specifies the delivery channel attributes:

```
{
  "name": "default",
  "s3BucketName": "config-bucket-123456789012",
  "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
  "configSnapshotDeliveryProperties": {
    "deliveryFrequency": "Twelve_Hours"
  }
}
```

This example sets the following attributes:

- `name` – The name of the delivery channel. By default, AWS Config assigns the name `default` to a new delivery channel.

You cannot update the delivery channel name with the `put-delivery-channel` command. For the steps to change the name, see [Renaming the Delivery Channel \(p. 58\)](#).

- `s3BucketName` – The name of the Amazon S3 bucket to which AWS Config delivers configuration snapshots and configuration history files.

If you specify a bucket that belongs to another AWS account, that bucket must have policies that grant access permissions to AWS Config. For more information, see [Permissions for the Amazon S3 Bucket \(p. 3292\)](#).

- `snsTopicARN` – The Amazon Resource Name (ARN) of the Amazon SNS topic to which AWS Config sends notifications about configuration changes.

If you choose a topic from another account, that topic must have policies that grant access permissions to AWS Config. For more information, see [Permissions for the Amazon SNS Topic \(p. 3295\)](#).

- `configSnapshotDeliveryProperties` – Contains the `deliveryFrequency` attribute, which sets how often AWS Config delivers configuration snapshots.

2. (Optional) You can use the `describe-delivery-channels` command to verify that the delivery channel settings are updated:

```
$ aws configservice describe-delivery-channels
{
  "DeliveryChannels": [
    {
      "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
      },
      "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
      "name": "default",
      "s3BucketName": "config-bucket-123456789012"
    }
  ]
}
```

## Renaming the Delivery Channel

To change the delivery channel name, you must delete it and create a new delivery channel with the desired name. Before you can delete the delivery channel, you must temporarily stop the configuration recorder.

The AWS Config console does not provide the option to delete the delivery channel, so you must use the AWS CLI, the AWS Config API, or one of the AWS SDKs.

### To rename the delivery channel (AWS CLI)

1. Use the `stop-configuration-recorder` command to stop the configuration recorder:

```
$ aws configservice stop-configuration-recorder --configuration-recorder-name configRecorderName
```

2. Use the `describe-delivery-channels` command, and take note of your delivery channel's attributes:

```
$ aws configservice describe-delivery-channels
{
  "DeliveryChannels": [
    {
      "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
      },
      "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
      "name": "default",
      "s3BucketName": "config-bucket-123456789012"
    }
  ]
}
```

3. Use the `delete-delivery-channel` command to delete the delivery channel:

```
$ aws configservice delete-delivery-channel --delivery-channel-name default
```

4. Use the `put-delivery-channel` command to create a delivery channel with the desired name:

```
$ aws configservice put-delivery-channel --delivery-channel file://deliveryChannel.json
```

The `deliveryChannel.json` file specifies the delivery channel attributes:

```
{
  "name": "myCustomDeliveryChannelName",
  "s3BucketName": "config-bucket-123456789012",
  "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
  "configSnapshotDeliveryProperties": {
    "deliveryFrequency": "Twelve_Hours"
  }
}
```

5. Use the `start-configuration-recorder` command to resume recording:

```
$ aws configservice start-configuration-recorder --configuration-recorder-name configRecorderName
```

## Updating the IAM Role Assigned to AWS Config

You can update the IAM role assumed by AWS Config any time. Before you update the IAM role, ensure that you have created a new role to replace the old one. You must attach policies to the new role that grant permissions to AWS Config to record configurations and deliver them to your delivery channel. In addition, make sure to copy the Amazon Resource Name (ARN) of your new IAM role. You will need it to update the IAM role. For information about creating an IAM role and attaching the required policies to the IAM role, see [Creating an IAM Role \(p. 29\)](#).

### Note

To find the ARN of an existing IAM role, go to the IAM console at <https://console.aws.amazon.com/iam/>. Choose **Roles** in the navigation pane. Then choose the name of the desired role and find the ARN at the top of the **Summary** page.

## Updating the IAM Role

You can update your IAM role using the AWS Management Console or the AWS CLI.

### To update the IAM role in a region where rules are supported (console)

If you are using AWS Config in a region that supports AWS Config rules, complete the following steps. For the list of supported regions, see [AWS Config Regions and Endpoints](#) in the *Amazon Web Services General Reference*.

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. Choose **Settings** in the navigation pane.
3. In the **AWS Config role**, section, choose the IAM role:
  - **Create a role** – AWS Config creates a role that has the required permissions. For **Role name**, you can customize the name that AWS Config creates.
  - **Choose a role from your account** – For **Role name**, choose an IAM role in your account. AWS Config will attach the required policies. For more information, see [Permissions for the IAM Role Assigned to AWS Config \(p. 3289\)](#).

### Note

Check the box if you want to use the IAM role as it. AWS Config will not attach policies to the role.

4. Choose **Save**.

### To update the IAM role in a region where rules are not supported (console)

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. On the **Resource inventory** page, choose the settings icon (⚙️).
3. Choose **Continue**.
4. In the **AWS Config is requesting permissions to read your resources' configuration** page, choose **View Details**.
5. In the **Role Summary** section, choose the IAM role:
  - If you want to create a role, for **IAM Role**, choose **Create a new IAM Role**. Then type a name for **Role Name**.
  - If you want to use an existing role, select it for **IAM Role**. Then, for **Policy Name**, select an available policy or create one by selecting **Create a new Role Policy**.

6. Choose **Allow**.

### To update the IAM role (AWS CLI)

- Use the `put-configuration-recorder` command and specify the Amazon Resource Name (ARN) of the new role:

```
$ aws configservice put-configuration-recorder --configuration-recorder  
name=configRecorderName,roleARN=arn:aws:iam::012345678912:role/myConfigRole
```

## Managing the Configuration Recorder

AWS Config uses the *configuration recorder* to detect changes in your resource configurations and capture these changes as configuration items. You must create a configuration recorder before AWS Config can track your resource configurations.

If you set up AWS Config by using the console or the AWS CLI, AWS Config automatically creates and then starts the configuration recorder for you. For more information, see [Getting Started With AWS Config \(p. 25\)](#).

By default, the configuration recorder records all supported resources in the region where AWS Config is running. You can create a customized configuration recorder that records only the resource types that you specify. For more information, see [Selecting Which Resources AWS Config Records \(p. 62\)](#).

You are charged service usage fees when AWS Config starts recording configurations. For pricing information, see [AWS Config Pricing](#). To control costs, you can stop recording by stopping the configuration recorder. After you stop recording, you can continue to access the configuration information that was already recorded. You will not be charged AWS Config usage fees until you resume recording.

When you start the configuration recorder, AWS Config takes an inventory of all AWS resources in your account.

## Managing the Configuration Recorder (Console)

You can use the AWS Config console to stop or start the configuration recorder.

### To stop or start the configuration recorder

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. Choose **Settings** in the navigation pane.
3. Stop or start the configuration recorder:
  - If you want to stop recording, under **Recording is on**, choose **Turn off**. When prompted, choose **Continue**.
  - If you want to start recording, under **Recording is off**, choose **Turn on**. When prompted, choose **Continue**.

## Managing the Configuration Recorder (AWS CLI)

You can use the AWS CLI to stop or start the configuration recorder. You can also rename or delete the configuration recorder using the AWS CLI, the AWS Config API, or one of the AWS SDKs. The following steps help you use the AWS CLI.

### To stop the configuration recorder

- Use the `stop-configuration-recorder` command:

```
$ aws configservice stop-configuration-recorder --configuration-recorder-  
name configRecorderName
```

### To start the configuration recorder

- Use the `start-configuration-recorder` command:

```
$ aws configservice start-configuration-recorder --configuration-recorder-  
name configRecorderName
```

### To rename the configuration recorder

To change the configuration recorder name, you must delete it and create a new configuration recorder with the desired name.

1. Use the `describe-configuration-recorders` command to look up the name of your current configuration recorder:

```
$ aws configservice describe-configuration-recorders  
{  
  "ConfigurationRecorders": [  
    {  
      "roleARN": "arn:aws:iam::012345678912:role/myConfigRole",  
      "name": "default"  
    }  
  ]  
}
```

2. Use the `delete-configuration-recorder` command to delete your current configuration recorder:

```
$ aws configservice delete-configuration-recorder --configuration-recorder-name default
```

3. Use the `put-configuration-recorder` command to create a configuration recorder with the desired name:

```
$ aws configservice put-configuration-recorder --configuration-recorder  
name=configRecorderName,roleARN=arn:aws:iam::012345678912:role/myConfigRole
```

4. Use the `start-configuration-recorder` command to resume recording:

```
$ aws configservice start-configuration-recorder --configuration-recorder-  
name configRecorderName
```

### To delete the configuration recorder

- Use the `delete-configuration-recorder` command:

```
$ aws configservice delete-configuration-recorder --configuration-recorder-name default
```

## Selecting Which Resources AWS Config Records

AWS Config continuously detects when any resource of a supported type is created, changed, or deleted. AWS Config records these events as configuration items. You can customize AWS Config to record changes for all supported types of resources or for only those types that are relevant to you. To learn which types of resources AWS Config can record, see [Supported Resource Types \(p. 9\)](#).

### Recording All Supported Resource Types

By default, AWS Config records the configuration changes for all supported types of *regional resources* that AWS Config discovers in the region in which it is running. Regional resources are tied to a region and can be used only in that region. Examples of regional resources are EC2 instances and EBS volumes.

You can also have AWS Config record supported types of *global resources*. Global resources are not tied to a specific region and can be used in all regions. The global resource types that AWS Config supports are IAM users, groups, roles, and customer managed policies.

#### **Important**

The configuration details for a specific global resource are the same in all regions. If you customize AWS Config in multiple regions to record global resources, AWS Config creates multiple configuration items each time a global resource changes: one configuration item for each region. These configuration items will contain identical data. To prevent duplicate configuration items, you should consider customizing AWS Config in only one region to record global resources, unless you want the configuration items to be available in multiple regions.

### Recording Specific Resource Types

If you don't want AWS Config to record the changes for all supported resources, you can customize it to record changes for only specific types. AWS Config records configuration changes for the types of resources that you specify, including the creation and deletion of such resources.

If a resource is not recorded, AWS Config captures only the creation and deletion of that resource, and no other details, at no cost to you. When a nonrecorded resource is created or deleted, AWS Config sends a notification, and it displays the event on the resource details page. The details page for a nonrecorded resource provides null values for most configuration details, and it does not provide information about relationships and configuration changes.

The relationship information that AWS Config provides for recorded resources is not limited because of missing data for nonrecorded resources. If a recorded resource is related to a nonrecorded resource, that relationship is provided in the details page of the recorded resource.

You can stop AWS Config from recording a type of resource any time. After AWS Config stops recording a resource, it retains the configuration information that was previously captured, and you can continue to access this information.

AWS Config rules can be used to evaluate compliance for only those resources that AWS Config records.

### Selecting Resources (Console)

You can use the AWS Config console to select the types of resources that AWS Config records.

#### **To select resources**

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. Open the **Settings** page:

- If you are using AWS Config in a region that supports AWS Config rules, choose **Settings** in the navigation pane. For the list of supported regions, see [AWS Config Regions and Endpoints](#) in the *Amazon Web Services General Reference*.
  - Otherwise, choose the settings icon (⚙️) on the **Resource inventory** page.
3. In the **Resource types to record** section, specify which types of AWS resources you want AWS Config to record:
    - **All resources** – AWS Config records all supported resources with the following options:
      - **Record all resources supported in this region** – AWS Config records configuration changes for every supported type of regional resource. When AWS Config adds support for a new type of regional resource, it automatically starts recording resources of that type.
      - **Include global resources** – AWS Config includes supported types of global resources with the resources that it records (for example, IAM resources). When AWS Config adds support for a new type of global resource, it automatically starts recording resources of that type.
    - **Specific types** – AWS Config records configuration changes for only those types of AWS resources that you specify.
  4. Save your changes:
    - If you are using AWS Config in a region that supports AWS Config rules, choose **Save**.
    - Otherwise, choose **Continue**. In the **AWS Config is requesting permissions to read your resources' configuration** page, choose **Allow**.

## Selecting Resources (AWS CLI)

You can use the AWS CLI to select the types of resources that you want AWS Config to record. You do this by creating a configuration recorder, which records the types of resources that you specify in a recording group. In the recording group, you specify whether all supported types or specific types of resources are recorded.

### To select all supported resources

1. Use the following `put-configuration-recorder` command:

```
$ aws configservice put-configuration-recorder --configuration-recorder
name=default,roleARN=arn:aws:iam::123456789012:role/config-role --recording-group
allSupported=true,includeGlobalResourceTypes=true
```

This command uses the following options for the `--recording-group` parameter:

- `allSupported=true` – AWS Config records configuration changes for every supported type of *regional resource*. When AWS Config adds support for a new type of regional resource, it automatically starts recording resources of that type.
- `includeGlobalResourceTypes=true` – AWS Config includes supported types of global resources with the resources that it records. When AWS Config adds support for a new type of global resource, it automatically starts recording resources of that type.

Before you can set this option to `true`, you must set the `allSupported` option to `true`.

If you do not want to include global resources, set this option to `false`, or omit it.

2. (Optional) To verify that your configuration recorder has the settings that you want, use the following `describe-configuration-recorders` command:

```
$ aws configservice describe-configuration-recorders
```

The following is an example response:

```
{
  "ConfigurationRecorders": [
    {
      "recordingGroup": {
        "allSupported": true,
        "resourceTypes": [],
        "includeGlobalResourceTypes": true
      },
      "roleARN": "arn:aws:iam::123456789012:role/config-role",
      "name": "default"
    }
  ]
}
```

### To select specific types of resources

1. Use the `aws configservice put-configuration-recorder` command, and pass one or more resource types through the `--recording-group` option, as shown in the following example:

```
$ aws configservice put-configuration-recorder --configuration-recorder
name=default,roleARN=arn:aws:iam::012345678912:role/myConfigRole --recording-
group file://recordingGroup.json
```

The `recordingGroup.json` file specifies which types of resources AWS Config will record:

```
{
  "allSupported": false,
  "includeGlobalResourceTypes": false,
  "resourceTypes": [
    "AWS:EC2:EIP",
    "AWS:EC2:Instance",
    "AWS:EC2:NetworkAcl",
    "AWS:EC2:SecurityGroup",
    "AWS:CloudTrail:Trail",
    "AWS:EC2:Volume",
    "AWS:EC2:VPC",
    "AWS:IAM:User",
    "AWS:IAM:Policy"
  ]
}
```

Before you can specify resource types for the `resourceTypes` key, you must set the `allSupported` and `includeGlobalResourceTypes` options to `false` or omit them.

2. (Optional) To verify that your configuration recorder has the settings that you want, use the following `describe-configuration-recorders` command:

```
$ aws configservice describe-configuration-recorders
```

The following is an example response:

```
{
  "ConfigurationRecorders": [
    {
      "recordingGroup": {
        "allSupported": false,
```

```
    "resourceTypes": [
      "AWS::EC2::EIP",
      "AWS::EC2::Instance",
      "AWS::EC2::NetworkAcl",
      "AWS::EC2::SecurityGroup",
      "AWS::CloudTrail::Trail",
      "AWS::EC2::Volume",
      "AWS::EC2::VPC",
      "AWS::IAM::User",
      "AWS::IAM::Policy"
    ],
    "includeGlobalResourceTypes": false
  },
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "name": "default"
}
]
```

## Recording Software Configuration for Managed Instances

You can use AWS Config to record software inventory changes on Amazon EC2 instances and on-premises servers. This enables you to see the historical changes to software configuration. For example, when a new Windows update is installed on a managed Windows instance, AWS Config records the changes and then sends the changes to your delivery channels, so that you are notified about the change. With AWS Config, you can see the history of when Windows updates were installed for the managed instance and how they changed over time.

You must complete the following steps to record software configuration changes:

- Turn on recording for the managed instance inventory resource type in AWS Config.
- Configure EC2 and on-premises servers as *managed instances* in AWS Systems Manager. A managed instance is a machine that has been configured for use with Systems Manager.
- Initiate collection of software inventory from your managed instances using the Systems Manager Inventory capability.

You can also use AWS Config rules to monitor software configuration changes and be notified whether the changes are compliant or noncompliant against your rules. For example, if you create a rule that checks whether your managed instances have a specified application, and an instance doesn't have that application installed, AWS Config flags that instance as noncompliant against your rule. For a list of AWS Config managed rules, see [List of AWS Config Managed Rules \(p. 103\)](#).

### To enable recording of software configuration changes in AWS Config:

1. Turn on recording for all supported resource types or selectively record the managed instance inventory resource type in AWS Config. For more information, see [Selecting Which Resources AWS Config Records \(p. 62\)](#).
2. Launch an Amazon EC2 instance with an instance profile for Systems Manager that includes the **AmazonSSMManagedInstanceCore** managed policy. This AWS managed policy enables an instance to use Systems Manager service core functionality.

For information about other policies you can add to the instance profile for Systems Manager, see [Create an IAM Instance Profile for Systems Manager](#) in the *AWS Systems Manager User Guide*.

### Important

SSM Agent is Amazon software that must be installed on a managed instance in order to communicate with the Systems Manager in the cloud. If your EC2 instance was created from an AMI for one of the following operating systems, the agent is preinstalled:

- Windows Server 2003-2012 R2 AMIs published in November 2016 or later
- Windows Server 2016 and 2019
- Amazon Linux
- Amazon Linux 2
- Ubuntu Server 16.04
- Ubuntu Server 18.04

On EC2 instances that were not created from an AMI with the agent preinstalled, you must install the agent manually. For information, see the following topics in the *AWS Systems Manager User Guide*:

- [Installing and Configuring SSM Agent on Windows Instances](#)
- [Installing and Configuring SSM Agent on Amazon EC2 Linux Instances](#)

3. Initiate inventory collection as described in [Configuring Inventory Collection](#) in the *AWS Systems Manager User Guide*. The procedures are the same for Linux and Windows instances.

AWS Config can record configuration changes for the following inventory types:

- **Applications** – A list of applications for managed instances, such as antivirus software.
- **AWS components** – A list of AWS components for managed instances, such as the AWS CLI and SDKs.
- **Instance information** – Instance information such as OS name and version, domain, and firewall status.
- **Network configuration** – Configuration information such as IP address, gateway, and subnet mask.
- **Windows Updates** – A list of Windows updates for managed instances (Windows instances only).

### Note

AWS Config doesn't support recording the custom inventory type at this time.

Inventory collection is one of many Systems Manager capabilities, which are grouped in the categories *Operations Management*, *Actions & Change*, *Instances & Nodes*, and *Shared Resources*. For more information, see [What is Systems Manager?](#) and [Systems Manager Capabilities](#) in the *AWS Systems Manager User Guide*.

## Querying the Current Configuration State of AWS Resources

You can use AWS Config to query the current configuration state of AWS resources based on configuration properties for a single account and Region or across multiple accounts and Regions. You can perform ad hoc, property-based queries against current AWS resource state metadata across all resources that AWS Config supports. The **advanced query** feature provides a single query endpoint and a powerful query language to get current resource state metadata without performing service-specific describe API calls. You can use configuration aggregators to run the same queries from a central account across multiple accounts and AWS Regions.

AWS Config uses a subset of structured query language (SQL) `SELECT` syntax to perform property-based queries and aggregations on the current configuration item (CI) data. The queries range in complexity from simple matches against tag and/or resource identifiers, to more complex queries, such as viewing all Amazon S3 buckets that have versioning disabled. This allows you to query exactly the current resource state you need without performing AWS service-specific API calls.

You can use advanced query for:

- Inventory management; for example, to retrieve a list of Amazon EC2 instances of a particular size.
- Security and operational intelligence; for example, to retrieve a list of resources that have a specific configuration property enabled or disabled.
- Cost optimization; for example, to identify a list of Amazon EBS volumes that are not attached to any EC2 instance.
- Compliance data; for example, to retrieve a list of all your conformance packs and their compliance status.

### Topics

- [Features \(p. 67\)](#)
- [Limitations \(p. 67\)](#)
- [Region Support \(p. 68\)](#)
- [Query Using the SQL Query Editor \(Console\) \(p. 70\)](#)
- [Query Using the SQL Query Editor \(AWS CLI\) \(p. 71\)](#)
- [Example Queries \(p. 74\)](#)
- [Example Relationship Queries \(p. 78\)](#)
- [Query Components \(p. 79\)](#)

## Features

The query language supports querying AWS resources based on CI properties of all AWS resource types supported by AWS Config, including configuration data, tags, and relationships. It is a subset of SQL `SELECT` command with limitations, as mentioned in the following section. It supports aggregation functions such as `AVG`, `COUNT`, `MAX`, `MIN`, and `SUM`.

## Limitations

As a subset of SQL `SELECT`, the query syntax has following limitations:

- No support for `ALL`, `AS`, `DISTINCT`, `FROM`, `HAVING`, `JOIN`, and `UNION` keywords in a query. `NULL` value queries are not supported.
- No support for querying on third-party resources. Third-party resources retrieved using advanced queries will have the configuration field set as `NULL`.
- No support for nested structures (such as tags) to be unpacked with SQL queries.
- When querying against multiple properties within an array of objects, matches are computed against all the array elements. For example, for a resource R with rules A and B, the resource is compliant to rule A but noncompliant to rule B. The resource R is stored as:

```
{
  configRuleList: [
    { configRuleName: 'A', complianceType: 'compliant' },
    { configRuleName: 'B', complianceType: 'non_compliant' }
  ]
}
```

R will be returned by this query:

```
SELECT configuration WHERE configuration.configRuleList.complianceType = 'non_compliant'
AND configuration.configRuleList.configRuleName = 'A'
```

The first condition `configuration.configRuleList.complianceType = 'non_compliant'` is applied to ALL elements in `R.configRuleList`, because R has a rule (rule B) with `complianceType = 'non_compliant'`, the condition is evaluated as true. The second condition `configuration.configRuleList.configRuleName` is applied to ALL elements in `R.configRuleList`, because R has a rule (rule A) with `configRuleName = 'A'`, the condition is evaluated as true. As both conditions are true, R will be returned.

- The `SELECT` all columns shorthand (that is `SELECT *`) selects only the top-level, scalar properties of a CI. The scalar properties returned are `accountId`, `awsRegion`, `arn`, `availabilityZone`, `configurationItemCaptureTime`, `resourceCreationTime`, `resourceId`, `resourceName`, `resourceType`, and `version`.
- Wildcard limitations:
  - Wildcards are supported only for property values and not for property keys (for example, `...WHERE someKey LIKE 'someValue%'` is supported but `...WHERE 'someKey%' LIKE 'someValue%'` is not supported).
  - Support for only suffix wildcards (for example, `...LIKE 'AWS::EC2::%'` is supported but `...LIKE '%::EC2::Instance'` is not supported).
  - Wildcard matches must be at least three characters long (for example, `...LIKE 'ab%'` is not allowed but `...LIKE 'abc%'` is allowed).
- Aggregation limitations:
  - Aggregate functions can accept only a single argument or property.
  - Aggregate functions cannot take other functions as arguments.
  - `GROUP BY` with an `ORDER BY` clause referencing aggregate functions may contain only a single property.
  - For all other aggregations `GROUP BY` clauses may contain up to three properties.
  - Pagination is supported for all aggregate queries except when `ORDER BY` clause has an aggregate function. For example, `GROUP BY X, ORDER BY Y` does not work if Y is an aggregate function.
  - No support for `HAVING` clauses in aggregations.

## Region Support

Advanced queries is supported in the following Regions:

Region name	Region	Endpoint	Protocol
Africa (Cape Town)*	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Middle East (Bahrain)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Asia Pacific (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asia Pacific (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS

Region name	Region	Endpoint	Protocol
Asia Pacific (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asia Pacific (Singapore)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pacific (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
AWS GovCloud (US-East)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (US-West)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS
Canada (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Europe (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europe (Ireland)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europe (London)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europe (Milan)*	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europe (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europe (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
South America (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
US West (N. California)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS

\*Saved queries is not available in Africa (Cape Town) and Europe (Milan) Regions.

\*Advanced queries for multi-account multi-regions is not available in Africa (Cape Town) and Europe (Milan) Regions.

## Query Using the SQL Query Editor (Console)

You can either use AWS sample queries or you can create your own query called as custom queries.

### Prerequisites

You must have permissions for `config:SelectResourceConfig` and `config:SelectAggregateResourceConfig` APIs. For more information, see [SelectResourceConfig API](#) and [SelectAggregateResourceConfig API](#).

You must have permissions for the `AWSConfigUserAccess` IAM managed policy. For more information, see [Granting Permissions for AWS Config Administration \(p. 3280\)](#).

If you are using `AWSServiceRoleForConfig` (service linked role) or `AWSConfigRole`, you will have permissions to save a query. If you are not using either of these roles, you must have permissions to `config:PutStoredQuery`, `config:GetStoredQuery`, `config:TagResource`, `config:UntagResource`, `config:ListTagsForResource` and `config:GetResources`.

### Use an AWS Sample Query

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. Choose **Advanced queries** from the left navigation to query your resource configurations for a single account and Region or for multiple accounts and Regions.
3. On the **Advanced queries** page, choose an appropriate query from the list of queries. You can filter a query either by the name, description, creator or tags. To filter AWS queries, choose **Creator** and enter **AWS**. The query is displayed in the SQL query editor. If required, you can edit this query.

#### Important

An updated list of properties and their data types is available in [GitHub](#).

#### Note

To run a query on an aggregator, create an aggregator. For more information, see [Setting Up an Aggregator Using the Console \(p. 3266\)](#). If you already have an aggregator set up, in the query scope, choose the aggregator to run an advanced query on that aggregator. When you select an aggregator, consider adding the AWS account ID and AWS Region in the query statement to view that information in the results.

4. To save this query to a new query, choose **Save As**.
  - In the **Query Name** field, update the name of the query.
  - In the **Description** field, update the description of the query.
  - Enter up to 50 unique tags for this query.
  - Choose **Save**.
5. Choose **Run**. The query results are displayed in the table below the query editor.
6. Choose **Export as** to export the query results in CSV or JSON format.

#### Note

The query results are paginated. When you choose export, upto 500 results are exported. You can also use the APIs to retrieve all the results. The results are paginated and you can retrieve 100 results at a time.

## Create your custom query

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. Choose **Advanced queries** from the left navigation to query your resource configurations for a single account and Region or for multiple accounts and Regions.
3. To create your custom query, choose **New query**.

### Important

An updated list of properties and their data types is available in [GitHub](#).

### Note

To view or edit a custom query, filter a query either by the name, description, creator or tags. To filter custom queries, choose **Creator** and enter **Custom**.

4. On the **Query editor** page, create your own query for this account and Region. You can also select an appropriate aggregator to create a query for multiple accounts and Regions.

### Note

To run a query on an aggregator, create an aggregator. For more information, see [Setting Up an Aggregator Using the Console \(p. 3266\)](#). If you already have an aggregator set up, in the query scope, choose the aggregator to run an advanced query on that aggregator. When you select an aggregator, consider adding the AWS account ID and AWS Region in the query statement to view that information in the results.

5. Edit if you wish you make changes to this query. Choose **Save Query** to save this query.
  - In the **Query Name** field, update the name of the query.
  - In the **Description** field, update the description of the query.
  - Enter up to 50 unique tags for this query.
  - Choose **Save**.
6. Choose **Run**. The query results are displayed in the table below the query editor.
7. Choose **Export as** to export the query results in CSV or JSON format.

### Note

The query results are paginated. When you choose export, upto 500 results are exported. You can also use the APIs to retrieve all the results. The results are paginated and you can retrieve 100 results at a time.

## Query Using the SQL Query Editor (AWS CLI)

To install the AWS Command Line Interface (AWS CLI) on your local computer, see [Installing the AWS CLI](#) in the *AWS CLI User Guide*.

### Query Resource Configuration Data

#### To query your resource configuration data using the query editor (AWS CLI) for a single account and Region

1. Open a command prompt or a terminal window.
2. Type the following command to query your resource configuration data.

```
aws configservice select-resource-config --expression "SELECT resourceId WHERE resourceType='AWS::EC2::Instance'"
```

Depending on your query, the output looks like the following.

```
{
  "QueryInfo": {
    "SelectFields": [
      {
        "Name": "resourceId"
      }
    ]
  },
  "Results": [
    {"resourceId": "ResourceId"},
    {"resourceId": "ResourceId"},
    {"resourceId": "ResourceId"},
    {"resourceId": "ResourceId"},
    {"resourceId": "ResourceId"},
    {"resourceId": "ResourceId"},
    {"resourceId": "ResourceId"}
  ]
}
```

### To query your resource configuration data using the query editor (AWS CLI) for multiple accounts and Regions

1. Open a command prompt or a terminal window.
2. Type the following command to query your resource configuration data.

```
aws configservice select-aggregate-resource-config --expression "SELECT resourceId
WHERE resourceType='AWS::EC2::Instance'" --configuration-aggregator-name my-aggregator
```

Depending on your query, the output looks like the following.

```
{
  "QueryInfo": {
    "SelectFields": [
      {
        "Name": "resourceId"
      }
    ]
  },
  "Results": [
    {"resourceId": "ResourceId"},
    {"resourceId": "ResourceId"},
    {"resourceId": "ResourceId"},
    {"resourceId": "ResourceId"},
    {"resourceId": "ResourceId"},
    {"resourceId": "ResourceId"},
    {"resourceId": "ResourceId"}
  ]
}
```

#### Note

While using the `AWS::IAM::User` resource type in an advanced query, use `awsRegion = 'global'`.

### Save a Query

1. Open a command prompt or a terminal window.
2. Type the following command to save a query.

```
aws configservice put-stored-query --stored-query '{"QueryName\": \"cli-test\",
  \"Expression\": \"SELECT *\", \"Description\": \"cli test query\" }'
  --tags '[{ \"Key\": \"first-tag\", \"Value\": \"\" }, { \"Key\": \"second-tag
  \", \"Value\": \"non-empty-tag-value\" }]'
```

3. Depending on your query, the output looks like the following.

```
{
  \"QueryArn\": \"arn:aws:config:eu-central-1:Account ID:stored-query/cli-test/query-
  e65mijt4rmam5pab\"
}
```

**Note**

--tags is optional. When you pass the tags, the saved tags will not be returned by either list-stored-queries or get-stored-query. You must use list-tag-for-resources to retrieve the associated tags for a saved query. --description is optional while creating or updating a query.

## View all the Saved Queries

1. Type the following command to view the list of all saved queries.

```
aws configservice list-stored-queries
```

2. Depending on your query, the output looks like the following.

```
{
  \"StoredQueryMetadata\": [
    {
      \"QueryId\": \"query-e65mijt4rmam5pab\",
      \"QueryArn\": \"arn:aws:config:eu-central-1:Account ID:stored-query/cli-test/
      query-e65mijt4rmam5pab\",
      \"QueryName\": \"cli-test\"
    },
    {
      \"QueryId\": \"query-rltwlewlqfivadxq\",
      \"QueryArn\": \"arn:aws:config:eu-central-1:Account ID:stored-query/cli-
      test-2/query-rltwlewlqfivadxq\",
      \"QueryName\": \"cli-test-2\",
      \"Description\": \"cli test query\"
    }
  ]
}
```

## Get Details of a Saved Query

1. Type the following command to get details of a specific saved query.

```
aws configservice get-stored-query --query-name cli-test
```

2. Depending on your query, the output looks like the following.

```
{
  \"StoredQuery\": {
    \"QueryId\": \"query-e65mijt4rmam5pab\",
```

```
    "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-test/  
query-e65mijt4rmam5pab",  
    "QueryName": "cli-test",  
    "Description": "cli test query",  
    "Expression": "SELECT *"  
  }  
}
```

## Delete a Saved Query

- Type the following command to delete your saved query.

```
aws configservice delete-stored-query --query-name cli-test
```

If successful, the command runs with no additional output.

## Example Queries

### Query to list all EC2 instances with AMI ID ami-12345

```
SELECT  
  resourceId,  
  resourceType,  
  configuration.instanceType,  
  configuration.placement.tenancy,  
  configuration.imageId,  
  availabilityZone  
WHERE  
  resourceType = 'AWS::EC2::Instance'  
  AND configuration.imageId = 'ami-12345'
```

### Results

```
{  
  "QueryInfo": {  
    "SelectFields": [  
      {  
        "Name": "resourceId"  
      },  
      {  
        "Name": "resourceType"  
      },  
      {  
        "Name": "configuration.instanceType"  
      },  
      {  
        "Name": "configuration.placement.tenancy"  
      },  
      {  
        "Name": "configuration.imageId"  
      },  
      {  
        "Name": "availabilityZone"  
      }  
    ]  
  },  
  "Results": [  

```

```

        {"resourceId":"resourceid","configuration":{"imageId":"ami-12345",
        \instanceType\":\"t2.micro\", \"placement\":{\"tenancy\":\"default\"}}, \"availabilityZone
        \": \"us-west-2c\", \"resourceType\":\"AWS::EC2::Instance\"},
        {"resourceId":"resourceid","configuration":{"imageId":"ami-12345",
        \instanceType\":\"t2.micro\", \"placement\":{\"tenancy\":\"default\"}}, \"availabilityZone
        \": \"us-west-2a\", \"resourceType\":\"AWS::EC2::Instance\"},
        {"resourceId":"resourceid","configuration":{"imageId":"ami-12345",
        \instanceType\":\"t2.micro\", \"placement\":{\"tenancy\":\"default\"}}, \"availabilityZone
        \": \"us-west-2c\", \"resourceType\":\"AWS::EC2::Instance\"},
        {"resourceId":"resourceid","configuration":{"imageId":"ami-12345\",
        \instanceType\":\"t1.micro\", \"placement\":{\"tenancy\":\"default\"}}, \"availabilityZone
        \": \"us-west-2a\", \"resourceType\":\"AWS::EC2::Instance\"},
        {"resourceId":"resourceid","configuration":{"imageId":"ami-12345\",
        \instanceType\":\"t2.micro\", \"placement\":{\"tenancy\":\"default\"}}, \"availabilityZone
        \": \"us-west-2c\", \"resourceType\":\"AWS::EC2::Instance\"},
        {"resourceId":"resourceid","configuration":{"imageId":"ami-12345\",
        \instanceType\":\"t2.micro\", \"placement\":{\"tenancy\":\"default\"}}, \"availabilityZone
        \": \"us-west-2c\", \"resourceType\":\"AWS::EC2::Instance\"},
        {"resourceId":"resourceid","configuration":{"imageId":"ami-12345\",
        \instanceType\":\"t2.micro\", \"placement\":{\"tenancy\":\"default\"}}, \"availabilityZone
        \": \"us-west-2c\", \"resourceType\":\"AWS::EC2::Instance\"}
    ]
}

```

### Query for count of resources grouped by their AWS Config rules compliance status

```

SELECT
    configuration.complianceType,
    COUNT(*)
WHERE
    resourceType = 'AWS::Config::ResourceCompliance'
GROUP BY
    configuration.complianceType

```

### Result

```

{
  "QueryInfo": {
    "SelectFields": [
      {
        "Name": "configuration.complianceType"
      },
      {
        "Name": "COUNT(*)"
      }
    ]
  },
  "Results": [
    {"COUNT(*)":163, "configuration":{"complianceType":"NON_COMPLIANT"}},
    {"COUNT(*)":2, "configuration":{"complianceType":"COMPLIANT"}}
  ]
}

```

### Query for the compliance status of AWS Conformance packs

```

SELECT
    resourceId,
    resourceName,
    resourceType,
    configuration.complianceType
WHERE
    resourceType = 'AWS::Config::ConformancePackCompliance'

```

Result

```
{
  "QueryInfo": {
    "SelectFields": [
      {
        "Name": "resourceId"
      },
      {
        "Name": "resourceName"
      },
      {
        "Name": "resourceType"
      },
      {
        "Name": "configuration.complianceType"
      }
    ]
  },
  "Results": [
    {"resourceId": "conformance-pack-conformance-pack-ID", "configuration": {"complianceType": "COMPLIANT"}, "resourceName": "MyConformancePack1", "resourceType": "AWS::Config::ConformancePackCompliance"},
    {"resourceId": "conformance-pack-conformance-pack-ID", "configuration": {"complianceType": "NON_COMPLIANT"}, "resourceName": "MyConformancePack2", "resourceType": "AWS::Config::ConformancePackCompliance"},
    {"resourceId": "conformance-pack-conformance-pack-ID", "configuration": {"complianceType": "NON_COMPLIANT"}, "resourceName": "MyConformancePack3", "resourceType": "AWS::Config::ConformancePackCompliance"}
  ]
}
```

Query to get counts of AWS resources grouped by account ID

```
aws configservice select-aggregate-resource-config --expression "SELECT COUNT(*), accountId group by accountId" --configuration-aggregator-name my-aggregator
```

Result

```
{
  "Results": [
    {"COUNT(*)": 2407, "accountId": "accountId"},
    {"COUNT(*)": 726, "accountId": "accountId"}
  ],
  "QueryInfo": {
    "SelectFields": [
      {
        "Name": "COUNT(*)"
      },
      {
        "Name": "accountId"
      }
    ]
  }
}
```

Query to list all EC2 volumes that are not in use

```
SELECT
  resourceId,
  accountId,
```

```
awsRegion,  
resourceType,  
configuration.volumeType,  
configuration.size,  
resourceCreationTime,  
tags,  
configuration.encrypted,  
configuration.availabilityZone,  
configuration.state.value  
WHERE  
  resourceType = 'AWS::EC2::Volume'  
AND  
  configuration.state.value <> 'in-use'
```

## Result

```
{  
  "Results": [  
    {"accountId": "accountId", "resourceId": "vol-0174de9c962f6581c", "awsRegion": "us-west-2", "configuration": {"volumeType": "gp2", "encrypted": false, "size": 100.0, "state": {"value": "available"}, "availabilityZone": "us-west-2a"}, "resourceCreationTime": "2020-02-21T07:39:43.771Z", "tags": [], "resourceType": "AWS::EC2::Volume"},  
    {"accountId": "accountId", "resourceId": "vol-0cbeb652a74af2f8f", "awsRegion": "us-east-1", "configuration": {"volumeType": "gp2", "encrypted": false, "size": 100.0, "state": {"value": "available"}, "availabilityZone": "us-east-1a"}, "resourceCreationTime": "2020-02-21T07:28:40.639Z", "tags": [], "resourceType": "AWS::EC2::Volume"},  
    {"accountId": "accountId", "resourceId": "vol-0a49952d528ec8ba2", "awsRegion": "ap-south-1", "configuration": {"volumeType": "gp2", "encrypted": false, "size": 100.0, "state": {"value": "available"}, "availabilityZone": "ap-south-1a"}, "resourceCreationTime": "2020-02-21T07:39:31.800Z", "tags": [], "resourceType": "AWS::EC2::Volume"},  
  ],  
  "QueryInfo": {  
    "SelectFields": [  
      {  
        "Name": "resourceId"  
      },  
      {  
        "Name": "accountId"  
      },  
      {  
        "Name": "awsRegion"  
      },  
      {  
        "Name": "resourceType"  
      },  
      {  
        "Name": "configuration.volumeType"  
      },  
      {  
        "Name": "configuration.size"  
      },  
      {  
        "Name": "resourceCreationTime"  
      },  
      {  
        "Name": "tags"  
      },  
      {  
        "Name": "configuration.encrypted"  
      },  
    ]  
  }  
}
```

```
        "Name": "configuration.availabilityZone"
      },
      {
        "Name": "configuration.state.value"
      }
    ]
  }
}
```

## Example Relationship Queries

Find EIPs related to an EC2 instance

```
SELECT
  resourceId
WHERE
  resourceType = 'AWS::EC2::EIP'
  AND relationships.resourceId = 'i-abcd1234'
```

Find EIPs related to an EC2 network interface

```
SELECT
  resourceId
WHERE
  resourceType = 'AWS::EC2::EIP'
  AND relationships.resourceId = 'eni-abcd1234'
```

Find EC2 instances and network interfaces related to a security group

```
SELECT
  resourceId
WHERE
  resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::NetworkInterface')
  AND relationships.resourceId = 'sg-abcd1234'
```

OR

```
SELECT
  resourceId
WHERE
  resourceType = 'AWS::EC2::Instance'
  AND relationships.resourceId = 'sg-abcd1234'

SELECT
  resourceId
WHERE
  resourceType = 'AWS::EC2::NetworkInterface'
  AND relationships.resourceId = 'sg-abcd1234'
```

Find EC2 instances, network ACLs, network interfaces and route tables related to a subnet

```
SELECT
  resourceId
WHERE
  resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::NetworkACL',
  'AWS::EC2::NetworkInterface', 'AWS::EC2::RouteTable')
  AND relationships.resourceId = 'subnet-abcd1234'
```

Find EC2 instances, internet gateways, network ACLs, network interfaces, route tables, subnets and security groups related to a VPC

```
SELECT
  resourceId
WHERE
  resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::InternetGateway',
  'AWS::EC2::NetworkACL', 'AWS::EC2::NetworkInterface', 'AWS::EC2::RouteTable',
  'AWS::EC2::Subnet', 'AWS::EC2::SecurityGroup')
  AND relationships.resourceId = 'vpc-abcd1234'
```

Find EC2 route tables related to a VPN gateway

```
SELECT
  resourceId
WHERE
  resourceType = 'AWS::EC2::RouteTable'
  AND relationships.resourceId = 'vgw-abcd1234'
```

## Query Components

The SQL `SELECT` query components are as follows.

### Synopsis

```
SELECT property [, ...]
[ WHERE condition ]
[ GROUP BY property ]
[ ORDER BY property [ ASC | DESC ] [, property [ ASC | DESC ] ...] ]
```

### Parameters

#### [ WHERE condition ]

Filters results according to the `condition` you specify.

#### [ GROUP BY property ]

Aggregates the result set into groups of rows with matching values for the given property.

The `GROUP BY` clause is applicable to aggregations. AWS Config supports grouping by only one property.

#### [ ORDER BY property [ ASC | DESC ] [, property [ ASC | DESC ] ...] ]

Sorts a result set by one or more output properties.

When the clause contains multiple properties, the result set is sorted according to the first property, then according to the second property for rows that have matching values for the first property, and so on.

### Examples

```
SELECT resourceId WHERE resourceType='AWS::EC2::Instance'
```

```
SELECT configuration.complianceType, COUNT(*) WHERE resourceType =
  'AWS::Config::ResourceCompliance' GROUP BY configuration.complianceType
```

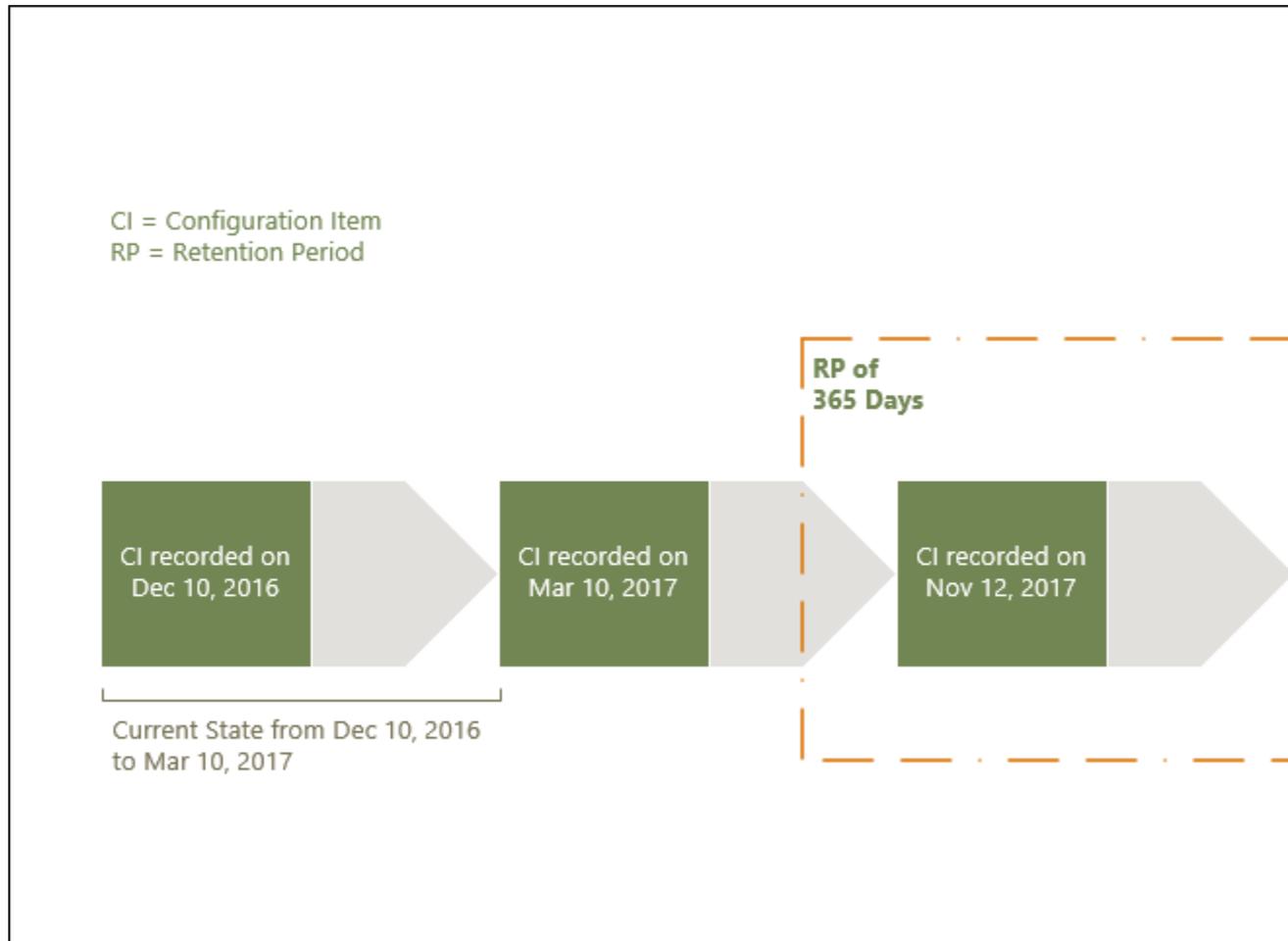
## Deleting AWS Config Data

AWS Config allows you to delete your data by specifying a retention period for your `ConfigurationItems`. When you specify a retention period, AWS Config retains your `ConfigurationItems` for that specified period. You can choose a period between a minimum of 30 days and a maximum of 7 years (2557 days). AWS Config deletes data older than your specified retention period. If you do not specify a retention period, AWS Config continues to store `ConfigurationItems` for the default period of 7 years (2557 days). When recording is switched on, the current state of the resource is when a `ConfigurationItem` is recorded and until the next change (a new `ConfigurationItem`) is recorded.

To understand the behavior of retention period, let's take a look at the timeline.

- When recording is switched on, the current state of a resource always exists and can't be deleted irrespective of the date the `ConfigurationItem` is recorded.
- When AWS Config records new `ConfigurationItems`, the previous `ConfigurationItems` are deleted depending on the specified retention period.

In the following timeline, AWS Config records `ConfigurationItems` at the following dates. For the purpose of this timeline, today is represented as May 24, 2018.



The following table explains which `ConfigurationItems` are displayed on the AWS Config timeline based on selected retention period.

Retention Period	Configuration Items displayed on timeline	Explanation
30 days	December 12, 2017	The current state of the resource started from December 12, 2017 when the <code>ConfigurationItem</code> was recorded and is valid until today (May 24, 2018). When recording is turned on, the current state always exists.
365 days	December 12, 2017; November 12, 2017, and March 10, 2017	<p>The retention period shows the current state December 12, 2017 and previous <code>ConfigurationItems</code> November 12, 2017 and March 10, 2017.</p> <p>The <code>ConfigurationItem</code> for March 10, 2017 is displayed on the timeline because that configuration state represented the current state 365 days ago.</p>

After you specify a retention period, AWS Config APIs no longer return `ConfigurationItems` that represent a state older than the specified retention period.

**Note**

- AWS Config cannot record your `ConfigurationItems` if recording is switched off.
- AWS Config cannot record your `ConfigurationItems` if your IAM role is broken.

## Setting Data Retention Period in AWS Management Console

In the AWS Management Console, if you do not select a data retention period, the default period is 7 years or 2557 days.

To set a custom data retention period for configuration items select the checkbox. You can select 1 year, 3 years, 5 years, or a custom period. For a custom period, enter the number of days between 30 and 2557 days.

## Resource types to record

Select the types of AWS resources for which you want AWS Config to record configuration changes. By default, AWS Config records configuration changes for all supported resources. You can also choose to record configuration changes for supported global resources.

- All resources**
- Record all resources supported in this region ⓘ
  - Include global resources (e.g., AWS IAM resources) ⓘ

**Specific types**

**Data retention period**

Default period is 7 years

- Set a custom retention period for configuration items recorded by AWS Config.

Custom

days

Select between a minimum period of 30 days and a maximum period of 7 years (2555 days).

## Notifications that AWS Config Sends to an Amazon SNS topic

You can configure AWS Config to stream configuration changes and notifications to an Amazon SNS topic. For example, when a resource is updated, you can get a notification sent to your email, so that you can view the changes. You can also be notified when AWS Config evaluates your custom or managed rules against your resources.

AWS Config sends notifications for the following events:

- Configuration item change for a resource.
- Configuration history for a resource was delivered for your account.
- Configuration snapshot for recorded resources was started and delivered for your account.
- Compliance state of your resources and whether they are compliant with your rules.
- Evaluation started for a rule against your resources.
- AWS Config failed to deliver the notification to your account.

### Topics

- [Example Configuration Item Change Notifications \(p. 83\)](#)
- [Example Configuration History Delivery Notification \(p. 90\)](#)
- [Example Configuration Snapshot Delivery Started Notification \(p. 91\)](#)
- [Example Configuration Snapshot Delivery Notification \(p. 91\)](#)
- [Example Compliance Change Notification \(p. 92\)](#)
- [Example Rules Evaluation Started Notification \(p. 93\)](#)
- [Example Oversized Configuration Item Change Notification \(p. 94\)](#)
- [Example Delivery Failed Notification \(p. 95\)](#)

## Example Configuration Item Change Notifications

AWS Config uses Amazon SNS to deliver notifications to subscription endpoints. These notifications provide the delivery status for configuration snapshots and configuration histories, and they provide each configuration item that AWS Config creates when the configurations of recorded AWS resources change. AWS Config also sends notifications that show whether your resources are compliant against your rules. If you choose to have notifications sent by email, you can use filters in your email client application based on the subject line and message body of the email.

The following is an example payload of an Amazon SNS notification that is generated when AWS Config detects that the Amazon Elastic Block Store volume `vol-ce676ccc` is attached to the instance with an ID of `i-344c463d`. The notification contains the configuration item change for the resource.

```
"Type": "Notification",
"MessageId": "8b945cb0-db34-5b72-b032-1724878af488",
"TopicArn": "arn:aws:sns:us-west-2:123456789012:example",
"Message": {
  "MessageVersion": "1.0",
  "NotificationCreateTime": "2014-03-18T10:11:00Z",
  "messageType": "ConfigurationItemChangeNotification",
  "configurationItems": [
    {
      "configurationItemVersion": "1.0",
      "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
      "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
      "resourceId": "vol-ce676ccc",
      "accountId": "123456789012",
      "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
      "configurationItemStatus": "OK",
      "relatedEvents": [],
      "availabilityZone": "us-west-2b",
      "resourceType": "AWS::EC2::VOLUME",
      "resourceCreationTime": "2014-02-27T21:43:53.885Z",
      "tags": {},
      "relationships": [
        {
          "resourceId": "i-344c463d",
          "resourceType": "AWS::EC2::INSTANCE",
          "name": "Attached to Instance"
        }
      ]
    },
    {
      "configuration": {
        "volumeId": "vol-ce676ccc",
        "size": 1,
        "snapshotId": "",
        "availabilityZone": "us-west-2b",
        "state": "in-use",
        "createTime": "2014-02-27T21:43:53.0885+0000",
        "attachments": [
          {
            "volumeId": "vol-ce676ccc",
            "instanceId": "i-344c463d",
            "device": "/dev/sdf",
            "state": "attached",
            "attachTime": "2014-03-07T23:46:28.0000+0000",
            "deleteOnTermination": false
          }
        ]
      },
      "tags": [],
      "volumeType": "standard"
    }
  ]
}
```

```

    ],
    "configurationItemDiff": {
      "changeType": "UPDATE",
      "changedProperties": {
        "Configuration.State": {
          "previousValue": "available",
          "updatedValue": "in-use",
          "changeType": "UPDATE"
        },
        "Configuration.Attachments.0": {
          "updatedValue": {
            "VolumeId": "vol-ce676ccc",
            "InstanceId": "i-344c463d",
            "Device": "/dev/sdf",
            "State": "attached",
            "AttachTime": "FriMar0723: 46: 28UTC2014",
            "DeleteOnTermination": "false"
          },
          "changeType": "CREATE"
        }
      }
    },
    "Timestamp": "2014-03-07T23:47:10.001Z",
    "SignatureVersion": "1",
    "Signature": "LgfJNB5aOk/w3omqsYrv5cUFY8yvIJvO5ZZh46/
    KGPAPk6HXRTBRLkhjacnXIXJEWSGI9mxvMmoWPLJGYEAR5FF/+/
    Ro9QTmiTNcEjQ5k8wGsRWRrk/whAzT2lVtofc365En2T1Ncd9iSFFXfJchgBmI7EACZ28t
    +n2mWFG057n6eGDvHTeds1zC6KxkfWTFXsR6zHXzkB3XuZImktflg3iPKtvBb3Zc9iVbNsBEI4FITFWktSqqomYDjc5h0kgapIo4CtC
    +qZhMzEbHWpzFLezvF155KaZXXDbznBD1ZkqPgno/WufuxszCiMrsmV8pUNUnkU1TA==",
    "SigningCertURL": "https://sns.us-west-2.amazonaws.com/SimpleNotificationService-
    e372f8ca30337fdb084e8ac449342c77.pem",
    "UnsubscribeURL": "https://sns.us-west-2.amazonaws.com/?
    Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
    west-2:123456789012:example:a6859fee-3638-407c-907e-879651c9d143"
  }
}

```

## Configuration Items for Resources with Relationships

If a resource is related to other resources, a change to that resource can result in multiple configuration items. The following example shows how AWS Config creates configuration items for resources with relationships.

1. You have an Amazon EC2 instance with an ID of `i-007d374c8912e3e90`, and the instance is associated with an Amazon EC2 security group, `sg-c8b141b4`.
2. You update your EC2 instance to change the security group to another security group, `sg-3f1fef43`.
3. Because the EC2 instance is related to another resource, AWS Config creates multiple configuration items like the following examples:

This notification contains the configuration item change for the EC2 instance when the security group is replaced.

```

{
  "Type": "Notification",
  "MessageId": "faeba85e-ef46-570a-b01c-f8b0faae8d5d",
  "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
  "Subject": "[AWS Config:us-east-2] AWS::EC2::Instance i-007d374c8912e3e90 Updated in Account 123456789012",
  "Message": {
    "configurationItemDiff": {

```

```
"changedProperties": {
  "Configuration.NetworkInterfaces.0": {
    "previousValue": {
      "networkInterfaceId": "eni-fde9493f",
      "subnetId": "subnet-2372be7b",
      "vpcId": "vpc-14400670",
      "description": "",
      "ownerId": "123456789012",
      "status": "in-use",
      "macAddress": "0e:36:a2:2d:c5:e0",
      "privateIpAddress": "172.31.16.84",
      "privateDnsName": "ip-172-31-16-84.ec2.internal",
      "sourceDestCheck": true,
      "groups": [{
        "groupName": "example-security-group-1",
        "groupId": "sg-c8b141b4"
      }],
      "attachment": {
        "attachmentId": "eni-attach-85bd89d9",
        "deviceIndex": 0,
        "status": "attached",
        "attachTime": "2017-01-09T19:36:02.000Z",
        "deleteOnTermination": true
      },
      "association": {
        "publicIp": "54.175.43.43",
        "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
        "ipOwnerId": "amazon"
      },
      "privateIpAddresses": [{
        "privateIpAddress": "172.31.16.84",
        "privateDnsName": "ip-172-31-16-84.ec2.internal",
        "primary": true,
        "association": {
          "publicIp": "54.175.43.43",
          "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
          "ipOwnerId": "amazon"
        }
      }
    ]
  },
  "updatedValue": null,
  "changeType": "DELETE"
},
"Relationships.0": {
  "previousValue": {
    "resourceId": "sg-c8b141b4",
    "resourceName": null,
    "resourceType": "AWS::EC2::SecurityGroup",
    "name": "Is associated with SecurityGroup"
  },
  "updatedValue": null,
  "changeType": "DELETE"
},
"Configuration.NetworkInterfaces.1": {
  "previousValue": null,
  "updatedValue": {
    "networkInterfaceId": "eni-fde9493f",
    "subnetId": "subnet-2372be7b",
    "vpcId": "vpc-14400670",
    "description": "",
    "ownerId": "123456789012",
    "status": "in-use",
    "macAddress": "0e:36:a2:2d:c5:e0",
    "privateIpAddress": "172.31.16.84",
    "privateDnsName": "ip-172-31-16-84.ec2.internal",
```

```

    "sourceDestCheck": true,
    "groups": [{
      "groupName": "example-security-group-2",
      "groupId": "sg-3f1fef43"
    }],
    "attachment": {
      "attachmentId": "eni-attach-85bd89d9",
      "deviceIndex": 0,
      "status": "attached",
      "attachTime": "2017-01-09T19:36:02.000Z",
      "deleteOnTermination": true
    },
    "association": {
      "publicIp": "54.175.43.43",
      "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
      "ipOwnerId": "amazon"
    },
    "privateIpAddresses": [{
      "privateIpAddress": "172.31.16.84",
      "privateDnsName": "ip-172-31-16-84.ec2.internal",
      "primary": true,
      "association": {
        "publicIp": "54.175.43.43",
        "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
        "ipOwnerId": "amazon"
      }
    }
  ]
},
"changeType": "CREATE"
},
"Relationships.1": {
  "previousValue": null,
  "updatedValue": {
    "resourceId": "sg-3f1fef43",
    "resourceName": null,
    "resourceType": "AWS::EC2::SecurityGroup",
    "name": "Is associated with SecurityGroup"
  },
  "changeType": "CREATE"
},
"Configuration.SecurityGroups.1": {
  "previousValue": null,
  "updatedValue": {
    "groupName": "example-security-group-2",
    "groupId": "sg-3f1fef43"
  },
  "changeType": "CREATE"
},
"Configuration.SecurityGroups.0": {
  "previousValue": {
    "groupName": "example-security-group-1",
    "groupId": "sg-c8b141b4"
  },
  "updatedValue": null,
  "changeType": "DELETE"
}
},
"changeType": "UPDATE"
},
"configurationItem": {
  "relatedEvents": [],
  "relationships": [
    {
      "resourceId": "eni-fde9493f",
      "resourceName": null,

```

```
        "resourceType": "AWS::EC2::NetworkInterface",
        "name": "Contains NetworkInterface"
    },
    {
        "resourceId": "sg-3f1fef43",
        "resourceName": null,
        "resourceType": "AWS::EC2::SecurityGroup",
        "name": "Is associated with SecurityGroup"
    },
    {
        "resourceId": "subnet-2372be7b",
        "resourceName": null,
        "resourceType": "AWS::EC2::Subnet",
        "name": "Is contained in Subnet"
    },
    {
        "resourceId": "vol-0a2d63a256bce35c5",
        "resourceName": null,
        "resourceType": "AWS::EC2::Volume",
        "name": "Is attached to Volume"
    },
    {
        "resourceId": "vpc-14400670",
        "resourceName": null,
        "resourceType": "AWS::EC2::VPC",
        "name": "Is contained in Vpc"
    }
],
"configuration": {
    "instanceId": "i-007d374c8912e3e90",
    "imageId": "ami-9be6f38c",
    "state": {
        "code": 16,
        "name": "running"
    },
    "privateDnsName": "ip-172-31-16-84.ec2.internal",
    "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
    "stateTransitionReason": "",
    "keyName": "ec2-micro",
    "amiLaunchIndex": 0,
    "productCodes": [],
    "instanceType": "t2.micro",
    "launchTime": "2017-01-09T20:13:28.000Z",
    "placement": {
        "availabilityZone": "us-east-2c",
        "groupName": "",
        "tenancy": "default",
        "hostId": null,
        "affinity": null
    },
    "kernelId": null,
    "ramdiskId": null,
    "platform": null,
    "monitoring": {"state": "disabled"},
    "subnetId": "subnet-2372be7b",
    "vpcId": "vpc-14400670",
    "privateIpAddress": "172.31.16.84",
    "publicIpAddress": "54.175.43.43",
    "stateReason": null,
    "architecture": "x86_64",
    "rootDeviceType": "ebs",
    "rootDeviceName": "/dev/xvda",
    "blockDeviceMappings": [{
        "deviceName": "/dev/xvda",
        "ebs": {
            "volumeId": "vol-0a2d63a256bce35c5",
```

AWS Config Developer Guide  
Example Configuration Item Change Notifications

---

```
        "status": "attached",
        "attachTime": "2017-01-09T19:36:03.000Z",
        "deleteOnTermination": true
    }
}],
"virtualizationType": "hvm",
"instanceLifecycle": null,
"spotInstanceRequestId": null,
"clientToken": "bIYqA1483990561516",
"tags": [{
    "key": "Name",
    "value": "value"
}],
"securityGroups": [{
    "groupName": "example-security-group-2",
    "groupId": "sg-3flfef43"
}],
"sourceDestCheck": true,
"hypervisor": "xen",
"networkInterfaces": [{
    "networkInterfaceId": "eni-fde9493f",
    "subnetId": "subnet-2372be7b",
    "vpcId": "vpc-14400670",
    "description": "",
    "ownerId": "123456789012",
    "status": "in-use",
    "macAddress": "0e:36:a2:2d:c5:e0",
    "privateIpAddress": "172.31.16.84",
    "privateDnsName": "ip-172-31-16-84.ec2.internal",
    "sourceDestCheck": true,
    "groups": [{
        "groupName": "example-security-group-2",
        "groupId": "sg-3flfef43"
    }],
    "attachment": {
        "attachmentId": "eni-attach-85bd89d9",
        "deviceIndex": 0,
        "status": "attached",
        "attachTime": "2017-01-09T19:36:02.000Z",
        "deleteOnTermination": true
    },
    "association": {
        "publicIp": "54.175.43.43",
        "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
        "ipOwnerId": "amazon"
    },
    "privateIpAddresses": [{
        "privateIpAddress": "172.31.16.84",
        "privateDnsName": "ip-172-31-16-84.ec2.internal",
        "primary": true,
        "association": {
            "publicIp": "54.175.43.43",
            "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
            "ipOwnerId": "amazon"
        }
    }
    ]
}],
"iamInstanceProfile": null,
"ebsOptimized": false,
"sriovNetSupport": null,
"enaSupport": true
},
"supplementaryConfiguration": {},
"tags": {"Name": "value"},
"configurationItemVersion": "1.2",
"configurationItemCaptureTime": "2017-01-09T22:50:14.328Z",
```

AWS Config Developer Guide  
Example Configuration Item Change Notifications

---

```
"configurationStateId": 1484002214328,
"awsAccountId": "123456789012",
"configurationItemStatus": "OK",
"resourceType": "AWS::EC2::Instance",
"resourceId": "i-007d374c8912e3e90",
"resourceName": null,
"ARN": "arn:aws:ec2:us-east-2:123456789012:instance/i-007d374c8912e3e90",
"awsRegion": "us-east-2",
"availabilityZone": "us-east-2c",
"configurationStateMd5Hash": "8d0f41750f5965e0071ae9be063ba306",
"resourceCreationTime": "2017-01-09T20:13:28.000Z"
},
"notificationCreationTime": "2017-01-09T22:50:15.928Z",
"messageType": "ConfigurationItemChangeNotification",
"recordVersion": "1.2"
},
"Timestamp": "2017-01-09T22:50:16.358Z",
"SignatureVersion": "1",
"Signature": "lpJTEYOSr8fUbiaaARNw1ECawJFVoD7I67mTeEkfAWJkqvvpak1ULHL1C
+IOsS/01A4P1Yci8GSK/coEC/O2XBntlw4CAtbMUgTQvb345Z2YZwcpK0kPNi6vN51DuZ/6DZA8EC
+gVTNT009xtNIH8aMlvqyvUSXuh278xayExC5yTRXEG+ikdZRd4QzS7obSK1kgRZWI6ipxPNL6rd56/
VvPxyhcbS7Vm40/2+e0nVb3bjNHBxjQTXSs1Xhuc9eP2gEsC4S132bGqdeDU1Y4dFGukuzPYoHuEtDPH
+GkLUq3KeiDAQshxAZLmOIRcQ7iJ/bELDjTN9AcX6lqLDZ79w==",
"SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
"UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

This notification contains the configuration item change for the EC2 security group, sg-3f1fef43, which is associated with the instance.

```
{
  "Type": "Notification",
  "MessageId": "564d873e-711e-51a3-b48c-d7d064f65bf4",
  "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
  "Subject": "[AWS Config:us-east-2] AWS::EC2::SecurityGroup sg-3f1fef43 Created in Account 123456789012",
  "Message": {
    "configurationItemDiff": {
      "changedProperties": {},
      "changeType": "CREATE"
    },
    "configurationItem": {
      "relatedEvents": [],
      "relationships": [{
        "resourceId": "vpc-14400670",
        "resourceName": null,
        "resourceType": "AWS::EC2::VPC",
        "name": "Is contained in Vpc"
      }],
      "configuration": {
        "ownerId": "123456789012",
        "groupName": "example-security-group-2",
        "groupId": "sg-3f1fef43",
        "description": "This is an example security group.",
        "ipPermissions": [],
        "ipPermissionsEgress": [{
          "ipProtocol": "-1",
          "fromPort": null,
          "toPort": null,
          "userIdGroupPairs": [],
          "ipRanges": ["0.0.0.0/0"],

```

```
        "prefixListIds": [],
      },
      "vpcId": "vpc-14400670",
      "tags": []
    },
    "supplementaryConfiguration": {},
    "tags": {},
    "configurationItemVersion": "1.2",
    "configurationItemCaptureTime": "2017-01-09T22:50:15.156Z",
    "configurationStateId": 1484002215156,
    "awsAccountId": "123456789012",
    "configurationItemStatus": "ResourceDiscovered",
    "resourceType": "AWS:EC2:SecurityGroup",
    "resourceId": "sg-3f1fef43",
    "resourceName": null,
    "ARN": "arn:aws:ec2:us-east-2:123456789012:security-group/sg-3f1fef43",
    "awsRegion": "us-east-2",
    "availabilityZone": "Not Applicable",
    "configurationStateMd5Hash": "7399608745296f67f7felc9ca56d5205",
    "resourceCreationTime": null
  },
  "notificationCreationTime": "2017-01-09T22:50:16.021Z",
  "messageType": "ConfigurationItemChangeNotification",
  "recordVersion": "1.2"
},
"Timestamp": "2017-01-09T22:50:16.413Z",
"SignatureVersion": "1",
"Signature": "GocX31Uu/zNFo85hZqzsNy30skwmLnjPjj+UjaJzkih
+dCP6gXYGQ0bK7uMzaLL2C/ibY0OsT7I/XY4NW6Amc5T46ydyHDjFRtQi8UfUQTqLXYRTnpOO/
hyK9lMFfhUNs4NwQpmx3n3mYEMpLuMs8DCgeBmB3AQ+hXPhNuNuR3mJVgo25S8AqphN900okZ2MKNUQy8iJm/
CVAx70TdnYsfUMZ24n88bUzAfiHGzc8QTthMdrFVUwXxa1h/7Zl8+A7BwoGmjo7W8CfLDVwaIQv1Uplgk3qd95Z0AXOzXVxNBQei4k8
"SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
"UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

## Example Configuration History Delivery Notification

The configuration history is a collection of the configuration items for a resource type over a time period. The following is an example notification that AWS Config sends when the configuration history for a CloudTrail trail resource is delivered for your account.

```
{
  "Type": "Notification",
  "MessageId": "ce49bf2c-d03a-51b0-8b6a-ef480a8b39fe",
  "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
  "Subject": "[AWS Config:us-east-2] Configuration History Delivery Completed for Account
123456789012",
  "Message": {
    "s3ObjectKey": "AWSLogs/123456789012/Config/us-
east-2/2016/9/27/ConfigHistory/123456789012_Config_us-
east-2_ConfigHistory_AWS::CloudTrail::Trail_20160927T195818Z_20160927T195818Z_1.json.gz",
    "s3Bucket": "config-bucket-123456789012-ohio",
    "notificationCreationTime": "2016-09-27T20:37:05.217Z",
    "messageType": "ConfigurationHistoryDeliveryCompleted",
    "recordVersion": "1.1"
  },
  "Timestamp": "2016-09-27T20:37:05.315Z",
  "SignatureVersion": "1",
```

```
"Signature": "OuIcS5RAKXTR6chQEJp3if4KJQV1Bz2kmXh7QE1/
RJQiCPsCNfG0J0rUZ1rqfKMqpps/Ka+zF0kg4dUCWV9PF0dliuwnjfbtYmDZpP4EBOoGmxcTliUn1Aie/
yeGFDuc6P3EotP3zt02rhmxjezjf3c11urstFZ8rTLVXp0z0xeyk4da0UetLsWZxUFEG0Z5uhk09mBo5dg/4mryIOovidhrbCBgX5ma
"SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
"UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

## Example Configuration Snapshot Delivery Started Notification

The following is an example notification that AWS Config sends when AWS Config starts delivering the configuration snapshot for your account.

```
{
  "Type": "Notification",
  "MessageId": "a32d0487-94b1-53f6-b4e6-5407c9c00be6",
  "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
  "Subject": "[AWS Config:us-east-2] Configuration Snapshot Delivery Started for Account
123456789012",
  "Message": {
    "configSnapshotId": "108e0794-84a7-4cca-a179-76a199ddd11a",
    "notificationCreationTime": "2016-10-18T17:26:09.572Z",
    "messageType": "ConfigurationSnapshotDeliveryStarted",
    "recordVersion": "1.1"
  },
  "Timestamp": "2016-10-18T17:26:09.840Z",
  "SignatureVersion": "1",
  "Signature": "BBA0DeKsfteTpYyZH5HPANpOLmW/jumOMBsgRq/kimY9tjNlkF/
V3BpLG1HVmDQdQzBh6oKE0h0rxcazbyGf5KF5W5r1zKK1EnS9xugFzALPUx//
olSj4neWallBkNIq1xvAQgu9qHfDR7dS2aCwe4scQfQjnlEv7PlZqxmt+ux3SR/
C54cbfcdUdpDsPwdo868+TpZvMtaU30ySnX04fmOgXoiA8AJO/EnjduQ08/zd4SYXhm+H9wavcWXB9XECeLhRW70Y
+wHQixfx40S1SaSRzvnJE+m9mHphFQs64YraRDRv6tMaenTk6CVPO+81ceAXIq2E1m7hZ71z4PA==",
  "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
  "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

## Example Configuration Snapshot Delivery Notification

The configuration snapshot is a collection of configuration items for all recorded resources and their configurations in your account. The following is an example notification that AWS Config sends when the configuration snapshot is delivered for your account.

```
{
  "Type": "Notification",
  "MessageId": "9fc82f4b-397e-5b69-8f55-7f2f86527100",
  "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
  "Subject": "[AWS Config:us-east-2] Configuration Snapshot Delivery Completed for
Account 123456789012",
  "Message": {
    "configSnapshotId": "16da64e4-cb65-4846-b061-e6c3ba43cb96",
  }
}
```

```
    "s3ObjectKey": "AWSLogs/123456789012/Config/us-east-2/2016/9/27/  
ConfigSnapshot/123456789012_Config_us-east-2_ConfigSnapshot_20160927T183939Z_16da64e4-  
cb65-4846-b061-e6c3ba43cb96.json.gz",  
    "s3Bucket": "config-bucket-123456789012-ohio",  
    "notificationCreationTime": "2016-09-27T18:39:39.853Z",  
    "messageType": "ConfigurationSnapshotDeliveryCompleted",  
    "recordVersion": "1.1"  
  },  
  "Timestamp": "2016-09-27T18:39:40.062Z",  
  "SignatureVersion": "1",  
  "Signature": "PMkWfUuj/fKIEXA7s2wTDLbZoF/MDsUkPspYghOpwu9n6m+C  
+zrm0cEZXPxxJPvhnWozG7SVqkHYf9QgI/diW2twP/HPDn5GQs2rNDc+YlaByEXnKVtHV1Gd4r1kN57E/  
oOW5NVLNczk5ymxAW+WGdptZJkCgyVuhJ28s08m3Z3Kqz96PPSxXzYZoCfCn/  
yP6CqXoN7olr4YCbYxYwn8zOUYcPmc45yYNSUTKzi+RJQRnDJKL2qb+s4h9w2fjbbBj8xe830VbFJqHhp7UkSfpc64Y  
+tRvmMLY5CI1cYrnuPRhTLdUk+ROsshg5G+JMtSLVG/TvWbjz44CKXJprjIQg==",  
  "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-  
b95095beb82e8f6a046b3aafc7f4149a.pem",  
  "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?  
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-  
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"  
}
```

## Example Compliance Change Notification

When AWS Config evaluates your resources against a custom or managed rule, AWS Config sends a notification that shows whether the resources are compliant against the rule.

The following is an example notification where the CloudTrail trail resource is compliant against the cloudtrail-enabled managed rule.

```
{  
  "Type": "Notification",  
  "MessageId": "11fd05dd-47e1-5523-bc01-55b988bb9478",  
  "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",  
  "Subject": "[AWS Config:us-east-2] AWS:::Account 123456789012 is COMPLIANT with  
cloudtrail-enabled in Accoun...",  
  "Message": {  
    "awsAccountId": "123456789012",  
    "configRuleName": "cloudtrail-enabled",  
    "configRuleARN": "arn:aws:config:us-east-2:123456789012:config-rule/config-  
rule-9rpvxc",  
    "resourceType": "AWS:::Account",  
    "resourceId": "123456789012",  
    "awsRegion": "us-east-2",  
    "newEvaluationResult": {  
      "evaluationResultIdentifier": {  
        "evaluationResultQualifier": {  
          "configRuleName": "cloudtrail-enabled",  
          "resourceType": "AWS:::Account",  
          "resourceId": "123456789012"  
        },  
        "orderingTimestamp": "2016-09-27T19:48:40.619Z"  
      },  
      "complianceType": "COMPLIANT",  
      "resultRecordedTime": "2016-09-27T19:48:41.405Z",  
      "configRuleInvokedTime": "2016-09-27T19:48:40.914Z",  
      "annotation": null,  
      "resultToken": null  
    },  
    "oldEvaluationResult": {  
      "evaluationResultIdentifier": {  
        "evaluationResultQualifier": {  
          "configRuleName": "cloudtrail-enabled",
```

```
    "resourceType": "AWS:::Account",
    "resourceId": "123456789012"
  },
  "orderingTimestamp": "2016-09-27T16:30:49.531Z"
},
"complianceType": "NON_COMPLIANT",
"resultRecordedTime": "2016-09-27T16:30:50.717Z",
"configRuleInvokedTime": "2016-09-27T16:30:50.105Z",
"annotation": null,
"resultToken": null
},
"notificationCreationTime": "2016-09-27T19:48:42.620Z",
"messageType": "ComplianceChangeNotification",
"recordVersion": "1.0"
},
"Timestamp": "2016-09-27T19:48:42.749Z",
"SignatureVersion": "1",
"Signature": "XZ9FfLb2ywkW9yJ0yBkNtIP5q7Cry6JtCEyUiHmG9gpOzi3seQ41udhtAqCZoiNiizAEi
+6gcttHCRVlhNemzp/
YmBmTfO6azYXt0FJDaeVd86k68VCS9aqRlBBjYlNo7ILi4Pqd5rE4BX2YBQSZcQyERgkUfTz2BIFyAmb1Q/
y4/6ez8rDyi545FDSLgcGEb4LKLNR6eDi4FbKtMGZHA7Nz8obqs1dHbgWYnp3c80mVll7ohP4hilcxdywAgXrbsN32ekYr15gdHozx8
+BIZ21ZtkcUtY5B3ImgRlUO7Yhn3L3c6rZxQ==",
  "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
  "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

## Example Rules Evaluation Started Notification

AWS Config sends a notification when it starts to evaluate your custom or managed rule against your resources. The following is an example notification when AWS Config starts to evaluate the `iam-password-policy` managed rule.

```
{
  "Type": "Notification",
  "MessageId": "358c8e65-e27a-594e-82d0-de1fe77393d7",
  "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
  "Subject": "[AWS Config:us-east-2] Config Rules Evaluation Started for Account
123456789012",
  "Message": {
    "awsAccountId": "123456789012",
    "awsRegion": "us-east-2",
    "configRuleNames": ["iam-password-policy"],
    "notificationCreationTime": "2016-10-13T21:55:21.339Z",
    "messageType": "ConfigRulesEvaluationStarted",
    "recordVersion": "1.0"
  },
  "Timestamp": "2016-10-13T21:55:21.575Z",
  "SignatureVersion": "1",
  "Signature": "DE431D+24zzFRboyPY2bPTsznJWe8L6TjDC+ItYllFkE9jACsBl3sQ1uSjYzEhEbN7Cs
+wBoHnJ/DxOSpyCxt4gigqKd+H2I636BvrQwHDhJwJm7qI6P8IozEliRvRWbM38zDTvHqkmmXQbdDHRsK/
MssMeVtBKuW0x8ivMrj+KpwuF57tE62eXeFhjBeJ0DKQV+aC+i3onsuT7HQvXQDBPDOM+cSuLrJamQJ6TcMU5G76qg/
gl494ilb4Vj4udboGwpHSgUvI3guFsc1SsTrlWXQKXabWtsCQPFdOhkKgmViCfMZrLRp8Pjnu
+uspYQELkEfwBchDVVzd15iMrAzQ==",
  "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
  "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

## Example Oversized Configuration Item Change Notification

When AWS Config detects a configuration change for a resource, it sends a configuration item notification. If the notification exceeds the maximum size allowed by Amazon Simple Notification Service (Amazon SNS), the notification includes a brief summary of the configuration item. You can view the complete notification in the Amazon S3 bucket location specified in the `s3BucketLocation` field.

The following example notification shows a configuration item for an Amazon EC2 instance. The notification includes a summary of the changes and the location of the notification in the Amazon S3 bucket.

```
View the Timeline for this Resource in AWS Config Management Console:
  https://console.aws.amazon.com/config/home?region=us-west-2#/timeline/
AWS::EC2::Instance/resourceId_14b76876-7969-4097-ab8e-a31942b02e80?
time=2016-10-06T16:46:16.261Z
```

The full configuration item change notification for this resource exceeded the maximum size allowed by Amazon Simple Notification Service (SNS). A summary of the configuration item is provided here. You can view the complete notification in the specified Amazon S3 bucket location.

New State Record Summary:

```
-----
{
  "configurationItemSummary": {
    "changeType": "UPDATE",
    "configurationItemVersion": "1.2",
    "configurationItemCaptureTime": "2016-10-06T16:46:16.261Z",
    "configurationStateId": 0,
    "awsAccountId": "123456789012",
    "configurationItemStatus": "OK",
    "resourceType": "AWS::EC2::Instance",
    "resourceId": "resourceId_14b76876-7969-4097-ab8e-a31942b02e80",
    "resourceName": null,
    "ARN": "arn:aws:ec2:us-west-2:123456789012:instance/resourceId_14b76876-7969-4097-
ab8e-a31942b02e80",
    "awsRegion": "us-west-2",
    "availabilityZone": null,
    "configurationStateMd5Hash": "8f1ee69b287895a0f8bc5753eca68e96",
    "resourceCreationTime": "2016-10-06T16:46:10.489Z"
  },
  "s3DeliverySummary": {
    "s3BucketLocation": "my-bucket/AWSLogs/123456789012/Config/
us-west-2/2016/10/6/OversizedChangeNotification/AWS::EC2::Instance/
resourceId_14b76876-7969-4097-ab8e-a31942b02e80/123456789012_Config_us-
west-2_ChangeNotification_AWS::EC2::Instance_resourceId_14b76876-7969-4097-ab8e-
a31942b02e80_20161006T164616Z_0.json.gz",
    "errorCode": null,
    "errorMessage": null
  },
  "notificationCreationTime": "2016-10-06T16:46:16.261Z",
  "messageType": "OversizedConfigurationItemChangeNotification",
  "recordVersion": "1.0"
}
```

## Example Delivery Failed Notification

AWS Config sends a delivery failed notification if AWS Config can't deliver the configuration snapshot or an oversized configuration item change notification to your Amazon S3 bucket. Verify that you specified a valid Amazon S3 bucket.

View the Timeline for this Resource in AWS Config Management Console:  
[https://console.aws.amazon.com/config/home?region=us-west-2#/timeline/AWS::EC2::Instance/test\\_resourceId\\_014b953d-75e3-40ce-96b9-c7240b975457?time=2016-10-06T16:46:13.749Z](https://console.aws.amazon.com/config/home?region=us-west-2#/timeline/AWS::EC2::Instance/test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457?time=2016-10-06T16:46:13.749Z)

The full configuration item change notification for this resource exceeded the maximum size allowed by Amazon Simple Notification Service (SNS). A summary of the configuration item is provided here. You can view the complete notification in the specified Amazon S3 bucket location.

New State Record Summary:

```
-----  
{  
  "configurationItemSummary": {  
    "changeType": "UPDATE",  
    "configurationItemVersion": "1.2",  
    "configurationItemCaptureTime": "2016-10-06T16:46:13.749Z",  
    "configurationStateId": 0,  
    "awsAccountId": "123456789012",  
    "configurationItemStatus": "OK",  
    "resourceType": "AWS::EC2::Instance",  
    "resourceId": "test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457",  
    "resourceName": null,  
    "ARN": "arn:aws:ec2:us-west-2:123456789012:instance/  
test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457",  
    "awsRegion": "us-west-2",  
    "availabilityZone": null,  
    "configurationStateMd5Hash": "6de64b95eacd30e7b63d4bba7cd80814",  
    "resourceCreationTime": "2016-10-06T16:46:10.489Z"  
  },  
  "s3DeliverySummary": {  
    "s3BucketLocation": null,  
    "errorCode": "NoSuchBucket",  
    "errorMessage": "Failed to deliver notification to bucket: bucket-example for  
account 123456789012 in region us-west-2."  
  },  
  "notificationCreationTime": "2016-10-06T16:46:13.749Z",  
  "messageType": "OversizedConfigurationItemChangeDeliveryFailed",  
  "recordVersion": "1.0"  
}
```

# Evaluating Resources with AWS Config Rules

Use AWS Config to evaluate the configuration settings of your AWS resources. You do this by creating AWS Config rules, which represent your ideal configuration settings. AWS Config provides customizable, predefined rules called managed rules to help you get started. While AWS Config continuously tracks the configuration changes that occur among your resources, it checks whether these changes violate any of the conditions in your rules. If a resource violates a rule, AWS Config flags the resource and the rule as *noncompliant*.

For example, when an EC2 volume is created, AWS Config can evaluate the volume against a rule that requires volumes to be encrypted. If the volume is not encrypted, AWS Config flags the volume and the rule as noncompliant. AWS Config can also check all of your resources for account-wide requirements. For example, AWS Config can check whether the number of EC2 volumes in an account stays within a desired total, or whether an account uses AWS CloudTrail for logging.

Service-linked rules are a unique type of managed rule that support other AWS services to create AWS Config rules in your account. These rules are predefined to include all the permissions required to call other AWS services on your behalf. These rules are similar to standards that an AWS service recommends in your AWS account for compliance verification. For more information, see [Service-Linked AWS Config Rules \(p. 3297\)](#).

The AWS Config console shows the compliance status of your rules and resources. You can see how your AWS resources comply overall with your desired configurations, and learn which specific resources are noncompliant. You can also use the AWS CLI, the AWS Config API, and AWS SDKs to make requests to the AWS Config service for compliance information.

By using AWS Config to evaluate your resource configurations, you can assess how well your resource configurations comply with internal practices, industry guidelines, and regulations.

For regions that support AWS Config rules, see [AWS Config Regions and Endpoints](#) in the *Amazon Web Services General Reference*.

You can create up to 150 AWS Config rules per region in your account. For more information, see [AWS Config Limits](#) in the *Amazon Web Services General Reference*.

You can also create custom rules to evaluate additional resources that AWS Config doesn't yet record. For more information, see [Evaluating Additional Resource Types \(p. 198\)](#).

## Topics

- [Region Support \(p. 97\)](#)
- [Viewing Configuration Compliance \(p. 98\)](#)
- [Specifying Triggers for AWS Config Rules \(p. 101\)](#)
- [AWS Config Managed Rules \(p. 102\)](#)
- [AWS Config Custom Rules \(p. 193\)](#)
- [Managing your AWS Config Rules \(p. 207\)](#)
- [Evaluating Your Resources \(p. 210\)](#)
- [Deleting Evaluation Results \(p. 211\)](#)
- [Enabling AWS Config Rules Across all Accounts in Your Organization \(p. 212\)](#)
- [Remediating Noncompliant AWS Resources by AWS Config Rules \(p. 213\)](#)
- [Tagging Your AWS Config Resources \(p. 217\)](#)

## Region Support

Currently, AWS Config Rules is supported in the following regions:

Region Name	Region	Endpoint	Protocol
Africa (Cape Town)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Middle East (Bahrain)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Asia Pacific (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asia Pacific (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia Pacific (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asia Pacific (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asia Pacific (Singapore)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pacific (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
AWS GovCloud (US-East)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (US-West)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS
Canada (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Europe (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europe (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europe (Ireland)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europe (London)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europe (Milan)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS

Region Name	Region	Endpoint	Protocol
Europe (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
South America (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
US West (N. California)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS

## Viewing Configuration Compliance

You can use the AWS Config console, AWS CLI, or AWS Config API to view the compliance state of your rules and resources.

### To view compliance (console)

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. In the AWS Management Console menu, verify that the region selector is set to a region that supports AWS Config rules. For the list of supported regions, see [AWS Config Regions and Endpoints](#) in the *Amazon Web Services General Reference*.
3. In the navigation pane, choose **Rules**. The console shows the **Rules** page, which lists your rules and the compliance status of each.
4. Choose a rule to view its **Rule details** page. This page shows the rule's configuration, its status, and any AWS resources that do not comply with it.
5. If the **Rule details** shows any noncompliant resources, choose the **Config timeline** icon () for a resource to see its configuration timeline page. The page shows the configuration settings that AWS Config captured when it detected that the resource was noncompliant. This information can help you determine why the resource fails to comply with the rule. For more information, see [Viewing Configuration Details](#) (p. 45).

You can also view the compliance of your resources by looking them up on the **Resource inventory** page. For more information, see [Looking Up Resources That Are Discovered by AWS Config](#) (p. 44).

### Example To view compliance (AWS CLI)

To view compliance, use any of the following CLI commands:

- To see the compliance state of each of your rules, use the `describe-compliance-by-config-rule` command, as shown in the following example:

```
$ aws configservice describe-compliance-by-config-rule
```

```
{
  "ComplianceByConfigRules": [
    {
      "Compliance": {
        "ComplianceContributorCount": {
          "CappedCount": 2,
          "CapExceeded": false
        },
        "ComplianceType": "NON_COMPLIANT"
      },
      "ConfigRuleName": "instances-in-vpc"
    },
    {
      "Compliance": {
        "ComplianceType": "COMPLIANT"
      },
      "ConfigRuleName": "restricted-common-ports"
    },
    ...
  ]
}
```

For each rule that has a compliance type of `NON_COMPLIANT`, AWS Config returns the number of noncompliant resources for the `CappedCount` parameter.

- To see the compliance state of each resource that AWS Config evaluates for a specific rule, use the [get-compliance-details-by-config-rule](#) command, as shown in the following example:

```
$ aws configservice get-compliance-details-by-config-rule --config-rule-
name ConfigRuleName{
  "EvaluationResults": [
    {
      "EvaluationResultIdentifier": {
        "OrderingTimestamp": 1443610576.349,
        "EvaluationResultQualifier": {
          "ResourceType": "AWS::EC2::Instance",
          "ResourceId": "i-nnnnnnnn",
          "ConfigRuleName": "ConfigRuleName"
        }
      },
      "ResultRecordedTime": 1443751424.969,
      "ConfigRuleInvokedTime": 1443751421.208,
      "ComplianceType": "COMPLIANT"
    },
    {
      "EvaluationResultIdentifier": {
        "OrderingTimestamp": 1443610576.349,
        "EvaluationResultQualifier": {
          "ResourceType": "AWS::EC2::Instance",
          "ResourceId": "i-nnnnnnnn",
          "ConfigRuleName": "ConfigRuleName"
        }
      },
      "ResultRecordedTime": 1443751425.083,
      "ConfigRuleInvokedTime": 1443751421.301,
      "ComplianceType": "NON_COMPLIANT"
    },
    ...
  ]
}
```

- To see the compliance state for each AWS resource of a specific type, use the [describe-compliance-by-resource](#) command, as shown in the following example:

```
$ aws configservice describe-compliance-by-resource --resource-type AWS::EC2::Instance
{
  "ComplianceByResources": [
    {

```

```
    "ResourceType": "AWS::EC2::Instance",
    "ResourceId": "i-nnnnnnnn",
    "Compliance": {
      "ComplianceContributorCount": {
        "CappedCount": 1,
        "CapExceeded": false
      },
      "ComplianceType": "NON_COMPLIANT"
    }
  },
  {
    "ResourceType": "AWS::EC2::Instance",
    "ResourceId": "i-nnnnnnnn",
    "Compliance": {
      "ComplianceType": "COMPLIANT"
    }
  },
  ...
```

- To see the compliance details of an individual AWS resource, use the `get-compliance-details-by-resource` command.

```
$ aws configservice get-compliance-details-by-resource --resource-type AWS::EC2::Instance
--resource-id i-nnnnnnnn
{
  "EvaluationResults": [
    {
      "EvaluationResultIdentifier": {
        "OrderingTimestamp": 1443610576.349,
        "EvaluationResultQualifier": {
          "ResourceType": "AWS::EC2::Instance",
          "ResourceId": "i-nnnnnnnn",
          "ConfigRuleName": "instances-in-vpc"
        }
      },
      "ResultRecordedTime": 1443751425.083,
      "ConfigRuleInvokedTime": 1443751421.301,
      "ComplianceType": "NON_COMPLIANT"
    }
  ]
}
```

### Example To view compliance (AWS Config API)

To view compliance, use any of the following API actions:

- To see the compliance state of each of your rules, use the [DescribeComplianceByConfigRule](#) action.
- To see the compliance state of each resource that AWS Config evaluates for a specific rule, use the [GetComplianceDetailsByConfigRule](#) action.
- To see the compliance state for each AWS resource of a specific type, use the [DescribeComplianceByResource](#) action.
- To see the compliance details of an individual AWS resource, use the [GetComplianceDetailsByResource](#) action. The details include which AWS Config rules evaluated the resource, when each rule last evaluated it, and whether the resource complies with each rule.

# Specifying Triggers for AWS Config Rules

When you add a rule to your account, you can specify when you want AWS Config to run the rule; this is called a *trigger*. AWS Config evaluates your resource configurations against the rule when the trigger occurs.

## Contents

- [Trigger types \(p. 101\)](#)
- [Example rules with triggers \(p. 101\)](#)
- [Rule evaluations when the configuration recorder is turned off \(p. 102\)](#)

## Trigger types

There are two types of triggers:

### Configuration changes

AWS Config runs evaluations for the rule when certain types of resources are created, changed, or deleted.

You choose which resources trigger the evaluation by defining the rule's *scope*. The scope can include the following:

- One or more resource types
- A combination of a resource type and a resource ID
- A combination of a tag key and value
- When any recorded resource is created, updated, or deleted

AWS Config runs the evaluation when it detects a change to a resource that matches the rule's scope. You can use the scope to constrain which resources trigger evaluations. Otherwise, evaluations are triggered when any recorded resource changes.

### Periodic

AWS Config runs evaluations for the rule at a frequency that you choose (for example, every 24 hours).

If you choose configuration changes and periodic, AWS Config invokes your Lambda function when it detects a configuration change and also at the frequency that you specify.

## Example rules with triggers

### Example rule with configuration change trigger

1. You add the AWS Config managed rule, `S3_BUCKET_LOGGING_ENABLED`, to your account to check whether your Amazon S3 buckets have logging enabled.
2. The trigger type for the rule is configuration changes. AWS Config runs the evaluations for the rule when an Amazon S3 bucket is created, changed, or deleted.
3. When a bucket is updated, the configuration change triggers the rule and AWS Config evaluates whether the bucket is compliant against the rule.

### Example rule with periodic trigger

1. You add the AWS Config managed rule, `IAM_PASSWORD_POLICY`, to your account. The rule checks whether the password policy for your IAM users comply with your account policy, such as requiring a minimum length or requiring specific characters.
2. The trigger type for the rule is periodic. AWS Config runs evaluation for the rule at a frequency that you specify, such as every 24 hours.
3. Every 24 hours, the rule is triggered and AWS Config evaluates whether the passwords for your IAM users are compliant against the rule.

### Example rule with configuration change and periodic triggers

1. You create a custom rule that evaluates whether CloudTrail trails in your account are turned on and logging for all regions.
2. You want AWS Config to run evaluations for the rule every time a trail is created, updated, or deleted. You also want AWS Config to run the rule every 12 hours.
3. For the trigger type, choose configuration changes and periodic.

## Rule evaluations when the configuration recorder is turned off

If you turn off the configuration recorder, AWS Config stops recording changes to your resource configurations. This affects your rule evaluations in the following ways:

- Rules with a periodic trigger continue to run evaluations at the specified frequency.
- Rules with a configuration change trigger do not run evaluations.
- Rules with both trigger types run evaluations only at the specified frequency. The rules do not run evaluations for configuration changes.
- If you run an on-demand evaluation for a rule with a configuration change trigger, the rule evaluates the last known state of the resource, which is the last recorded configuration item.

## AWS Config Managed Rules

AWS Config provides *AWS managed rules*, which are predefined, customizable rules that AWS Config uses to evaluate whether your AWS resources comply with common best practices. For example, you could use a managed rule to quickly start assessing whether your Amazon Elastic Block Store (Amazon EBS) volumes are encrypted or whether specific tags are applied to your resources. You can set up and activate these rules without writing the code to create an AWS Lambda function, which is required if you want to create custom rules. The AWS Config console guides you through the process of configuring and activating a managed rule. You can also use the AWS Command Line Interface or AWS Config API to pass the JSON code that defines your configuration of a managed rule.

You can customize the behavior of a managed rule to suit your needs. For example, you can define the rule's scope to constrain which resources trigger an evaluation for the rule, such as EC2 instances or volumes. You can customize the rule's parameters to define attributes that your resources must have to comply with the rule. For example, you can customize a parameter to specify that your security group should block incoming traffic to a specific port number.

After you activate a rule, AWS Config compares your resources to the conditions of the rule. After this initial evaluation, AWS Config continues to run evaluations each time one is triggered. The evaluation triggers are defined as part of the rule, and they can include the following types:

- **Configuration changes** – AWS Config triggers the evaluation when any resource that matches the rule's scope changes in configuration. The evaluation runs after AWS Config sends a configuration item change notification.
- **Periodic** – AWS Config runs evaluations for the rule at a frequency that you choose (for example, every 24 hours).

The AWS Config console shows which resources comply with the rule and which rules are being followed. For more information, see [Viewing Configuration Compliance \(p. 98\)](#).

#### Topics

- [List of AWS Config Managed Rules \(p. 103\)](#)
- [Working with AWS Config Managed Rules \(p. 191\)](#)
- [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#)

## List of AWS Config Managed Rules

AWS Config currently supports the following managed rules in the analytics; compute; cryptography and PKI; database; machine learning; management and governance; migration and transfer; network and content delivery; security; identity and compliance; and storage categories.

#### Topics

- [access-keys-rotated \(p. 107\)](#)
- [account-part-of-organizations \(p. 108\)](#)
- [acm-certificate-expiration-check \(p. 108\)](#)
- [alb-http-drop-invalid-header-enabled \(p. 109\)](#)
- [alb-http-to-https-redirect-check \(p. 109\)](#)
- [alb-waf-enabled \(p. 109\)](#)
- [api-gw-cache-enabled-and-encrypted \(p. 110\)](#)
- [api-gw-endpoint-type-check \(p. 110\)](#)
- [api-gw-execution-logging-enabled \(p. 111\)](#)
- [api-gw-ssl-enabled \(p. 111\)](#)
- [api-gw-xray-enabled \(p. 111\)](#)
- [approved-amis-by-id \(p. 112\)](#)
- [approved-amis-by-tag \(p. 112\)](#)
- [aurora-mysql-backtracking-enabled \(p. 113\)](#)
- [autoscaling-group-elb-healthcheck-required \(p. 113\)](#)
- [beanstalk-enhanced-health-reporting-enabled \(p. 113\)](#)
- [cloudformation-stack-drift-detection-check \(p. 114\)](#)
- [cloudformation-stack-notification-check \(p. 114\)](#)
- [cloudfront-accesslogs-enabled \(p. 115\)](#)
- [cloudfront-associated-with-waf \(p. 115\)](#)
- [cloudfront-custom-ssl-certificate \(p. 116\)](#)
- [cloudfront-default-root-object-configured \(p. 116\)](#)
- [cloudfront-origin-access-identity-enabled \(p. 116\)](#)
- [cloudfront-origin-failover-enabled \(p. 117\)](#)
- [cloudfront-sni-enabled \(p. 117\)](#)

- [cloudfront-viewer-policy-https](#) (p. 117)
- [cloudtrail-s3-dataevents-enabled](#) (p. 118)
- [cloudtrail-security-trail-enabled](#) (p. 118)
- [cloudwatch-alarm-action-check](#) (p. 119)
- [cloudwatch-alarm-resource-check](#) (p. 120)
- [cloudwatch-alarm-settings-check](#) (p. 120)
- [cloudwatch-log-group-encrypted](#) (p. 121)
- [cloud-trail-cloud-watch-logs-enabled](#) (p. 121)
- [cloudtrail-enabled](#) (p. 121)
- [cloud-trail-encryption-enabled](#) (p. 122)
- [cloud-trail-log-file-validation-enabled](#) (p. 122)
- [cmk-backing-key-rotation-enabled](#) (p. 123)
- [codebuild-project-envvar-awscred-check](#) (p. 123)
- [codebuild-project-source-repo-url-check](#) (p. 123)
- [codepipeline-deployment-count-check](#) (p. 124)
- [codepipeline-region-fanout-check](#) (p. 124)
- [cw-loggroup-retention-period-check](#) (p. 125)
- [dax-encryption-enabled](#) (p. 125)
- [db-instance-backup-enabled](#) (p. 126)
- [desired-instance-tenancy](#) (p. 126)
- [desired-instance-type](#) (p. 127)
- [dms-replication-not-public](#) (p. 127)
- [dynamodb-autoscaling-enabled](#) (p. 128)
- [dynamodb-in-backup-plan](#) (p. 128)
- [dynamodb-pitr-enabled](#) (p. 129)
- [dynamodb-table-encrypted-kms](#) (p. 129)
- [dynamodb-table-encryption-enabled](#) (p. 129)
- [dynamodb-throughput-limit-check](#) (p. 130)
- [ebs-in-backup-plan](#) (p. 130)
- [ebs-optimized-instance](#) (p. 131)
- [ebs-snapshot-public-restorable-check](#) (p. 131)
- [ec2-ebs-encryption-by-default](#) (p. 131)
- [ec2-imdsv2-check](#) (p. 132)
- [ec2-instance-detailed-monitoring-enabled](#) (p. 132)
- [ec2-instance-managed-by-systems-manager](#) (p. 132)
- [ec2-instance-no-public-ip](#) (p. 133)
- [ec2-instance-profile-attached](#) (p. 133)
- [ec2-managedinstance-applications-blacklisted](#) (p. 134)
- [ec2-managedinstance-applications-required](#) (p. 134)
- [ec2-managedinstance-association-compliance-status-check](#) (p. 135)
- [ec2-managedinstance-inventory-blacklisted](#) (p. 135)
- [ec2-managedinstance-patch-compliance-status-check](#) (p. 136)

- [ec2-managedinstance-platform-check](#) (p. 136)
- [ec2-security-group-attached-to-eni](#) (p. 137)
- [ec2-stopped-instance](#) (p. 137)
- [ec2-volume-inuse-check](#) (p. 137)
- [ecs-task-definition-user-for-host-mode-check](#) (p. 138)
- [efs-encrypted-check](#) (p. 138)
- [efs-in-backup-plan](#) (p. 139)
- [eip-attached](#) (p. 139)
- [eks-endpoint-no-public-access](#) (p. 139)
- [eks-secrets-encrypted](#) (p. 140)
- [elasticache-redis-cluster-automatic-backup-check](#) (p. 140)
- [elasticache-redis-cluster-auto-backup-check](#) (p. 141)
- [elasticsearch-encrypted-at-rest](#) (p. 141)
- [elasticsearch-in-vpc-only](#) (p. 141)
- [elasticsearch-node-to-node-encryption-check](#) (p. 142)
- [elastic-beanstalk-managed-updates-enabled](#) (p. 142)
- [elb-acm-certificate-required](#) (p. 143)
- [elb-cross-zone-load-balancing-enabled](#) (p. 143)
- [elb-custom-security-policy-ssl-check](#) (p. 143)
- [elb-deletion-protection-enabled](#) (p. 144)
- [elb-logging-enabled](#) (p. 144)
- [elb-predefined-security-policy-ssl-check](#) (p. 145)
- [elb-tls-https-listeners-only](#) (p. 145)
- [emr-kerberos-enabled](#) (p. 145)
- [emr-master-no-public-ip](#) (p. 146)
- [encrypted-volumes](#) (p. 146)
- [fms-security-groups-audit-policy-check](#) (p. 147)
- [fms-security-groups-content-check](#) (p. 148)
- [fms-security-groups-resource-association-check](#) (p. 148)
- [fms-shield-resource-policy-check](#) (p. 149)
- [fms-webacl-resource-policy-check](#) (p. 150)
- [fms-webacl-rulegroup-association-check](#) (p. 151)
- [guardduty-enabled-centralized](#) (p. 152)
- [guardduty-non-archived-findings](#) (p. 152)
- [iam-customer-policy-blocked-kms-actions](#) (p. 153)
- [iam-group-has-users-check](#) (p. 153)
- [iam-inline-policy-blocked-kms-actions](#) (p. 153)
- [iam-no-inline-policy-check](#) (p. 154)
- [iam-password-policy](#) (p. 154)
- [iam-policy-blacklisted-check](#) (p. 155)
- [iam-policy-in-use](#) (p. 155)
- [iam-policy-no-statements-with-admin-access](#) (p. 156)

- [iam-role-managed-policy-check](#) (p. 157)
- [iam-root-access-key-check](#) (p. 157)
- [iam-user-group-membership-check](#) (p. 157)
- [iam-user-mfa-enabled](#) (p. 158)
- [iam-user-no-policies-check](#) (p. 158)
- [iam-user-unused-credentials-check](#) (p. 159)
- [restricted-ssh](#) (p. 159)
- [ec2-instances-in-vpc](#) (p. 159)
- [internet-gateway-authorized-vpc-only](#) (p. 160)
- [kms-cmk-not-scheduled-for-deletion](#) (p. 160)
- [lambda-concurrency-check](#) (p. 161)
- [lambda-dlq-check](#) (p. 161)
- [lambda-function-public-access-prohibited](#) (p. 161)
- [lambda-function-settings-check](#) (p. 162)
- [lambda-inside-vpc](#) (p. 162)
- [mfa-enabled-for-iam-console-access](#) (p. 163)
- [multi-region-cloudtrail-enabled](#) (p. 163)
- [no-unrestricted-route-to-igw](#) (p. 164)
- [rds-automatic-minor-version-upgrade-enabled](#) (p. 164)
- [rds-cluster-deletion-protection-enabled](#) (p. 164)
- [rds-cluster-iam-authentication-enabled](#) (p. 165)
- [rds-enhanced-monitoring-enabled](#) (p. 165)
- [rds-instance-deletion-protection-enabled](#) (p. 166)
- [rds-instance-iam-authentication-enabled](#) (p. 166)
- [rds-instance-public-access-check](#) (p. 166)
- [rds-in-backup-plan](#) (p. 167)
- [rds-logging-enabled](#) (p. 167)
- [rds-multi-az-support](#) (p. 168)
- [rds-snapshots-public-prohibited](#) (p. 168)
- [rds-snapshot-encrypted](#) (p. 168)
- [rds-storage-encrypted](#) (p. 169)
- [redshift-backup-enabled](#) (p. 169)
- [redshift-cluster-configuration-check](#) (p. 170)
- [redshift-cluster-kms-enabled](#) (p. 170)
- [redshift-cluster-maintenancesettings-check](#) (p. 171)
- [redshift-cluster-public-access-check](#) (p. 171)
- [redshift-enhanced-vpc-routing-enabled](#) (p. 171)
- [redshift-require-tls-ssl](#) (p. 172)
- [required-tags](#) (p. 172)
- [restricted-common-ports](#) (p. 174)
- [root-account-hardware-mfa-enabled](#) (p. 175)
- [root-account-mfa-enabled](#) (p. 175)

- [s3-account-level-public-access-blocks](#) (p. 175)
- [s3-bucket-blacklisted-actions-prohibited](#) (p. 176)
- [s3-bucket-default-lock-enabled](#) (p. 177)
- [s3-bucket-level-public-access-prohibited](#) (p. 177)
- [s3-bucket-logging-enabled](#) (p. 177)
- [s3-bucket-policy-grantee-check](#) (p. 178)
- [s3-bucket-policy-not-more-permissive](#) (p. 179)
- [s3-bucket-public-read-prohibited](#) (p. 179)
- [s3-bucket-public-write-prohibited](#) (p. 180)
- [s3-bucket-replication-enabled](#) (p. 180)
- [s3-bucket-server-side-encryption-enabled](#) (p. 181)
- [s3-bucket-ssl-requests-only](#) (p. 181)
- [s3-bucket-versioning-enabled](#) (p. 181)
- [s3-default-encryption-kms](#) (p. 182)
- [sagemaker-endpoint-configuration-kms-key-configured](#) (p. 182)
- [sagemaker-notebook-instance-kms-key-configured](#) (p. 183)
- [sagemaker-notebook-no-direct-internet-access](#) (p. 183)
- [secretsmanager-rotation-enabled-check](#) (p. 183)
- [secretsmanager-scheduled-rotation-success-check](#) (p. 184)
- [secretsmanager-secret-periodic-rotation](#) (p. 184)
- [secretsmanager-secret-unused](#) (p. 185)
- [secretsmanager-using-cmk](#) (p. 185)
- [securityhub-enabled](#) (p. 186)
- [service-vpc-endpoint-enabled](#) (p. 186)
- [shield-advanced-enabled-autorenew](#) (p. 186)
- [shield-drt-access](#) (p. 187)
- [sns-encrypted-kms](#) (p. 187)
- [subnet-auto-assign-public-ip-disabled](#) (p. 188)
- [vpc-default-security-group-closed](#) (p. 188)
- [vpc-flow-logs-enabled](#) (p. 188)
- [vpc-network-acl-unused-check](#) (p. 189)
- [vpc-sg-open-only-to-authorized-ports](#) (p. 189)
- [vpc-vpn-2-tunnels-up](#) (p. 189)
- [wafv2-logging-enabled](#) (p. 190)
- [waf-classic-logging-enabled](#) (p. 190)

## access-keys-rotated

Checks if the active access keys are rotated within the number of days specified in `maxAccessKeyAge`. The rule is `NON_COMPLIANT` if the access keys have not been rotated for more than `maxAccessKeyAge` number of days.

**Note**

Re-evaluating this rule within 4 hours of the first evaluation will have no effect on the results.

**Identifier:** ACCESS\_KEYS\_ROTATED

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

maxAccessKeyAge, Type: int, Default: 90

Maximum number of days without rotation. Default 90.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## account-part-of-organizations

Checks if an AWS account is part of AWS Organizations. The rule is NON\_COMPLIANT if an AWS account is not part of AWS Organizations or AWS Organizations master account ID does not match rule parameter `MasterAccountId`.

**Identifier:** ACCOUNT\_PART\_OF\_ORGANIZATIONS

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing) Region

**Parameters:**

MasterAccountId (Optional), Type: String

The master account ID for an AWS account.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## acm-certificate-expiration-check

Checks if AWS Certificate Manager Certificates in your account are marked for expiration within the specified number of days. Certificates provided by ACM are automatically renewed. ACM does not automatically renew certificates that you import.

**Identifier:** ACM\_CERTIFICATE\_EXPIRATION\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), China (Ningxia), Europe (Milan) Region

**Parameters:**

daysToExpiration (Optional), Type: int, Default: 14

Specify the number of days before the rule flags the ACM Certificate as noncompliant.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## alb-http-drop-invalid-header-enabled

Checks if rule evaluates AWS Application Load Balancers (ALB) to ensure they are configured to drop http headers. The rule is NON\_COMPLIANT if the value of routing.http.drop\_invalid\_header\_fields.enabled is set to false.

**Identifier:** ALB\_HTTP\_DROP\_INVALID\_HEADER\_ENABLED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## alb-http-to-https-redirection-check

Checks whether HTTP to HTTPS redirection is configured on all HTTP listeners of Application Load Balancers. The rule is NON\_COMPLIANT if one or more HTTP listeners of Application Load Balancer do not have HTTP to HTTPS redirection configured.

**Identifier:** ALB\_HTTP\_TO\_HTTPS\_REDIRECTION\_CHECK

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## alb-waf-enabled

Checks if Web Application Firewall (WAF) is enabled on Application Load Balancers (ALBs). This rule is NON\_COMPLIANT if key: waf.enabled is set to false.

**Identifier:** ALB\_WAF\_ENABLED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), China (Ningxia), AWS GovCloud (US-East), AWS GovCloud (US-West), Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

wafWebAclIds (Optional), Type: CSV

Comma separated list of web ACL ID (for WAF) or web ACL ARN (for WAFV2) checking for ALB association.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## api-gw-cache-enabled-and-encrypted

Checks that all methods in Amazon API Gateway stages have cache enabled and cache encrypted. The rule is NON\_COMPLIANT if any method in Amazon API Gateway stage is not configured to cache or the cache is not encrypted.

**Identifier:** API\_GW\_CACHE\_ENABLED\_AND\_ENCRYPTED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## api-gw-endpoint-type-check

Checks if Amazon API Gateway APIs are of the type specified in the rule parameter `endpointConfigurationType`. The rule returns NON\_COMPLIANT if the REST API does not match the endpoint type configured in the rule parameter.

**Identifier:** API\_GW\_ENDPOINT\_TYPE\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

endpointConfigurationTypes, Type: String

Comma-separated list of allowed endpointConfigurationTypes. Allowed values are REGIONAL, PRIVATE and EDGE.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

### api-gw-execution-logging-enabled

Checks that all methods in Amazon API Gateway stage has logging enabled. The rule is NON\_COMPLIANT if logging is not enabled. The rule is NON\_COMPLIANT if `loggingLevel` is neither ERROR nor INFO.

**Identifier:** API\_GW\_EXECUTION\_LOGGING\_ENABLED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

`loggingLevel` (Optional), Type: String, Default: ERROR,INFO

Comma-separated list of specific logging levels (for example, ERROR, INFO or ERROR,INFO).

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

### api-gw-ssl-enabled

Checks if a REST API stage uses an Secure Sockets Layer (SSL) certificate. This rule is NON\_COMPLIANT if the REST API stage does not have an associated SSL certificate.

**Identifier:** API\_GW\_SSL\_ENABLED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

`CertificateIDs` (Optional), Type: CSV

Comma-separated list of client certificate IDs configured on a REST API stage.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

### api-gw-xray-enabled

Checks if X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule will return COMPLIANT if X-Ray tracing is enabled, NON\_COMPLIANT otherwise.

**Identifier:** API\_GW\_XRAY\_ENABLED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## approved-amis-by-id

Checks if running instances are using specified AMIs. Specify a list of approved AMI IDs. Running instances with AMIs that are not on this list are NON\_COMPLIANT.

**Identifier:** APPROVED\_AMIS\_BY\_ID

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

amilds, Type: CSV

The AMI IDs (comma-separated list of up to 10).

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## approved-amis-by-tag

Checks if running instances are using specified AMIs. Specify a list of approved AMI IDs. Running instances with AMIs that are not on this list are NON\_COMPLIANT.

**Identifier:** APPROVED\_AMIS\_BY\_TAG

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

amisByTagKeyAndValue, Type: StringMap, Default: tag-key:tag-value,other-tag-key

The AMIs by tag (comma-separated list up to 10; for example,tag-key:tag-value; i.e. tag-key1 matches AMIs with tag-key1,tag-key2:value2 matches tag-key2 having value2).

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## aurora-mysql-backtracking-enabled

Checks if an Amazon Aurora MySQL cluster has backtracking enabled. This rule is NON\_COMPLIANT if the Aurora cluster uses MySQL and it does not have backtracking enabled.

**Identifier:** AURORA\_MYSQL\_BACKTRACKING\_ENABLED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), China (Ningxia), Asia Pacific (Hong Kong), Europe (Milan), Europe (Stockholm), Middle East (Bahrain), Africa (Cape Town), South America (Sao Paulo) Region

**Parameters:**

BacktrackWindowInHours (Optional), Type: double

Amount of time in hours (up to 72) to backtrack your Aurora MySQL cluster.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## autoscaling-group-elb-healthcheck-required

Checks whether your Auto Scaling groups that are associated with a load balancer are using Elastic Load Balancing health checks.

**Identifier:** AUTOSCALING\_GROUP\_ELB\_HEALTHCHECK\_REQUIRED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## beanstalk-enhanced-health-reporting-enabled

Checks if an AWS Elastic Beanstalk environment is configured for enhanced health reporting. The rule is COMPLIANT if the environment is configured for enhanced health reporting. The rule is NON\_COMPLIANT if the environment is configured for basic health reporting.

**Identifier:** BEANSTALK\_ENHANCED\_HEALTH\_REPORTING\_ENABLED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## cloudformation-stack-drift-detection-check

Checks if the actual configuration of a Cloud Formation stack differs, or has drifted, from the expected configuration. A stack is considered to have drifted if one or more of its resources differ from their expected configuration. The rule and the stack are COMPLIANT when the stack drift status is IN\_SYNC. The rule and the stack are NON\_COMPLIANT when the stack drift status is DRIFTED.

**Identifier:** CLOUDFORMATION\_STACK\_DRIFT\_DETECTION\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), China (Ningxia), AWS GovCloud (US-East), AWS GovCloud (US-West), Asia Pacific (Hong Kong), Asia Pacific (Osaka), Europe (Milan), Europe (Paris), Europe (Stockholm), Middle East (Bahrain), Africa (Cape Town) Region

**Parameters:**

cloudformationRoleArn, Type: String

The AWS CloudFormation role ARN with IAM policy permissions to detect drift for AWS CloudFormation Stacks

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## cloudformation-stack-notification-check

Checks whether your CloudFormation stacks are sending event notifications to an SNS topic. Optionally checks whether specified SNS topics are used.

**Identifier:** CLOUDFORMATION\_STACK\_NOTIFICATION\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), China (Ningxia), AWS GovCloud (US-East), AWS GovCloud (US-West), Asia Pacific (Hong Kong), Asia Pacific (Osaka), Europe (Milan), Europe (Paris), Europe (Stockholm), Middle East (Bahrain), Africa (Cape Town) Region

**Parameters:**

snsTopic1 (Optional), Type: String

SNS Topic ARN.

snsTopic2 (Optional), Type: String

SNS Topic ARN.

snsTopic3 (Optional), Type: String

SNS Topic ARN.

snsTopic4 (Optional), Type: String

SNS Topic ARN.

snsTopic5 (Optional), Type: String

SNS Topic ARN.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## cloudfront-accesslogs-enabled

Checks if Amazon CloudFront distributions are configured to capture information from Amazon Simple Storage Service (Amazon S3) server access logs. This rule is NON\_COMPLIANT if a CloudFront distribution does not have logging configured.

**Identifier:** CLOUDFRONT\_ACCESSLOGS\_ENABLED

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (N. Virginia), Asia Pacific (Osaka) Region

**Parameters:**

S3BucketName (Optional), Type: String

The name of the Amazon S3 bucket for storing server access logs.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## cloudfront-associated-with-waf

Checks if Amazon CloudFront distributions are associated with either WAF or WAFv2 web access control lists (ACLs). This rule is NON\_COMPLIANT if a CloudFront distribution is not associated with a web ACL.

**Identifier:** CLOUDFRONT\_ASSOCIATED\_WITH\_WAF

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (N. Virginia), Asia Pacific (Osaka) Region

**Parameters:**

wafWebAclIds (Optional), Type: CSV

Comma-separated list of web ACL IDs for WAF or web ACL Amazon Resource Names (ARNs) for WAFV2.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## cloudfront-custom-ssl-certificate

Checks if the certificate associated with an Amazon CloudFront distribution is the default Secure Sockets Layer (SSL) certificate. This rule is NON\_COMPLIANT if a CloudFront distribution uses the default SSL certificate.

**Identifier:** CLOUDFRONT\_CUSTOM\_SSL\_CERTIFICATE

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (N. Virginia), Asia Pacific (Osaka) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## cloudfront-default-root-object-configured

Checks if an Amazon CloudFront distribution is configured to return a specific object that is the default root object. The rule is NON\_COMPLIANT if Amazon CloudFront distribution does not have a default root object configured.

**Identifier:** CLOUDFRONT\_DEFAULT\_ROOT\_OBJECT\_CONFIGURED

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## cloudfront-origin-access-identity-enabled

Checks if Amazon CloudFront distribution with S3 Origin type has Origin Access Identity (OAI) configured. The rule is NON\_COMPLIANT if the CloudFront distribution is backed by S3 and any of S3 Origin type is not OAI configured. The rule is NON\_COMPLIANT if the origin is not an S3 bucket; the rule does not return NOT\_APPLICABLE if the origin is not as S3 bucket.

**Identifier:** CLOUDFRONT\_ORIGIN\_ACCESS\_IDENTITY\_ENABLED

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## cloudfront-origin-failover-enabled

Checks whether an origin group is configured for the distribution of at least 2 origins in the origin group for Amazon CloudFront. This rule is NON\_COMPLIANT if there are no origin groups for the distribution.

**Identifier:** CLOUDFRONT\_ORIGIN\_FAILOVER\_ENABLED

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## cloudfront-sni-enabled

Checks if Amazon CloudFront distributions are using a custom SSL certificate and are configured to use SNI to serve HTTPS requests. This rule is NON\_COMPLIANT if a custom SSL certificate is associated but the SSL support method is a dedicated IP address.

**Identifier:** CLOUDFRONT\_SNI\_ENABLED

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## cloudfront-viewer-policy-https

Checks whether your Amazon CloudFront distributions use HTTPS (directly or via a redirection). The rule is NON\_COMPLIANT if the value of ViewerProtocolPolicy is set to 'allow-all' for the defaultCacheBehavior or for the cacheBehaviors.

**Identifier:** CLOUDFRONT\_VIEWER\_POLICY\_HTTPS

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## cloudtrail-s3-dataevents-enabled

Checks whether at least one AWS CloudTrail trail is logging Amazon S3 data events for all S3 buckets. The rule is NON\_COMPLIANT if trails log data events for S3 buckets is not configured.

**Identifier:** CLOUDTRAIL\_S3\_DATAEVENTS\_ENABLED

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

S3BucketNames (Optional), Type: String

Comma-separated list of S3 bucket names for which data events logging should be enabled. Default behavior checks for all S3 buckets.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## cloudtrail-security-trail-enabled

Checks that there is at least one AWS CloudTrail trail defined with security best practices. This rule is COMPLIANT if there is at least one trail that meets all of the following:

- records global service events
- is a multi-region trail
- has Log file validation enabled
- encrypted with a KMS key
- records events for reads and writes
- records management events
- does not exclude any management events

This rule is NON\_COMPLIANT if no trails meet all of the criteria mentioned above.

**Identifier:** CLOUDTRAIL\_SECURITY\_TRAIL\_ENABLED

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## cloudwatch-alarm-action-check

Checks whether CloudWatch alarms have at least one alarm action, one INSUFFICIENT\_DATA action, or one OK action enabled. Optionally, checks whether any of the actions matches one of the specified ARNs.

**Identifier:** CLOUDWATCH\_ALARM\_ACTION\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

alarmActionRequired, Type: String, Default: true

Alarms have at least one action.

insufficientDataActionRequired, Type: String, Default: true

Alarms have at least one action when the alarm transitions to the INSUFFICIENT\_DATA state from any other state.

okActionRequired, Type: String, Default: false

Alarms have at least one action when the alarm transitions to an OK state from any other state.

action1 (Optional), Type: String

The action to execute, specified as an ARN.

action2 (Optional), Type: String

The action to execute, specified as an ARN.

action3 (Optional), Type: String

The action to execute, specified as an ARN.

action4 (Optional), Type: String

The action to execute, specified as an ARN.

action5 (Optional), Type: String

The action to execute, specified as an ARN.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## cloudwatch-alarm-resource-check

Checks whether the specified resource type has a CloudWatch alarm for the specified metric. For resource type, you can specify EBS volumes, EC2 instances, RDS clusters, or S3 buckets.

**Identifier:** CLOUDWATCH\_ALARM\_RESOURCE\_CHECK

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

resourceType, Type: String

AWS resource type. The value can be one of the following: `AWS::EC2::Volume`, `AWS::EC2::Instance`, `AWS::RDS::DBCluster`, or `AWS::S3::Bucket`.

metricName, Type: String

The name for the metric associated with the alarm (for example, 'CPUUtilization' for EC2 instances).

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## cloudwatch-alarm-settings-check

Checks whether CloudWatch alarms with the given metric name have the specified settings.

**Identifier:** CLOUDWATCH\_ALARM\_SETTINGS\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

metricName, Type: String

The name for the metric associated with the alarm.

threshold (Optional), Type: int

The value against which the specified statistic is compared.

evaluationPeriods (Optional), Type: int

The number of periods over which data is compared to the specified threshold.

period (Optional), Type: int, Default: 300

The period, in seconds, during which the specified statistic is applied.

comparisonOperator (Optional), Type: String

The operation for comparing the specified statistic and threshold (for example, 'GreaterThanThreshold').

statistic (Optional), Type: String

The statistic for the metric associated with the alarm (for example, 'Average' or 'Sum').

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

### cloudwatch-log-group-encrypted

Checks if a log group in Amazon CloudWatch Logs is encrypted with a AWS Key Management Service (KMS) managed Customer Master Keys (CMK). The rule is NON\_COMPLIANT if no AWS KMS CMK is configured on the log groups.

**Identifier:** CLOUDWATCH\_LOG\_GROUP\_ENCRYPTED

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), China (Ningxia) Region

**Parameters:**

KmsKeyId (Optional), Type: String

Amazon Resource Name (ARN) of AWS Key Management Service (KMS) key that is used to encrypt the CloudWatch Logs log group.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

### cloud-trail-cloud-watch-logs-enabled

Checks whether AWS CloudTrail trails are configured to send logs to Amazon CloudWatch logs. The trail is non-compliant if the CloudWatchLogsLogGroupArn property of the trail is empty.

**Identifier:** CLOUD\_TRAIL\_CLOUD\_WATCH\_LOGS\_ENABLED

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

expectedDeliveryWindowAge (Optional), Type: int

Maximum age in hours of the most recent delivery to CloudWatch logs that satisfies compliance.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

### cloudtrail-enabled

Checks if AWS CloudTrail is enabled in your AWS account. Optionally, you can specify which S3 bucket, SNS topic, and AWS CloudTrail ARN to use.

**Identifier:** CLOUD\_TRAIL\_ENABLED

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

s3BucketName (Optional), Type: String

Name of S3 bucket for CloudTrail to deliver log files to.

snsTopicArn (Optional), Type: String

SNS topic ARN for CloudTrail to use for notifications.

cloudWatchLogsLogGroupArn (Optional), Type: String

CloudWatch log group ARN for CloudTrail to send data to.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## cloud-trail-encryption-enabled

Checks whether AWS CloudTrail is configured to use the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master key (CMK) encryption. The rule is compliant if the KmsKeyId is defined.

**Identifier:** CLOUD\_TRAIL\_ENCRYPTION\_ENABLED

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## cloud-trail-log-file-validation-enabled

Checks whether AWS CloudTrail creates a signed digest file with logs. AWS recommends that the file validation must be enabled on all trails. The rule is noncompliant if the validation is not enabled.

**Identifier:** CLOUD\_TRAIL\_LOG\_FILE\_VALIDATION\_ENABLED

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## cmk-backing-key-rotation-enabled

Checks if key rotation is enabled for each key and matches to the key ID of the customer created customer master key (CMK). The rule is COMPLIANT, if the key rotation is enabled for specific key object. The rule is not applicable to CMKs that have imported key material.

**Note**

This rule only evaluates symmetric AWS KMS; keys and ignores asymmetric AWS KMS keys.

**Identifier:** CMK\_BACKING\_KEY\_ROTATION\_ENABLED

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## codebuild-project-envvar-awscred-check

Checks whether the project contains environment variables AWS\_ACCESS\_KEY\_ID and AWS\_SECRET\_ACCESS\_KEY. The rule is NON\_COMPLIANT when the project environment variables contains plaintext credentials.

**Identifier:** CODEBUILD\_PROJECT\_ENVVAR\_AWSCRED\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except AWS GovCloud (US-East), Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## codebuild-project-source-repo-url-check

Checks whether the GitHub or Bitbucket source repository URL contains either personal access tokens or user name and password. The rule is complaint with the usage of OAuth to grant authorization for accessing GitHub or Bitbucket repositories.

**Identifier:** CODEBUILD\_PROJECT\_SOURCE\_REPO\_URL\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except AWS GovCloud (US-East), Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## codepipeline-deployment-count-check

Checks whether the first deployment stage of the AWS Codepipeline performs more than one deployment. Optionally checks if each of the subsequent remaining stages deploy to more than the specified number of deployments (`deploymentLimit`).

**Identifier:** CODEPIPELINE\_DEPLOYMENT\_COUNT\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), China (Ningxia), AWS GovCloud (US-East), AWS GovCloud (US-West), Asia Pacific (Hong Kong), Asia Pacific (Osaka), Europe (Milan), Europe (Stockholm), Middle East (Bahrain), Africa (Cape Town) Region

**Parameters:**

`deploymentLimit` (Optional), Type: int

The maximum number of deployments each stage can perform.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## codepipeline-region-fanout-check

Checks if each stage in the AWS CodePipeline deploys to more than N times the number of the regions the AWS CodePipeline has deployed in all the previous combined stages, where N is the region fanout number. The first deployment stage can deploy to a maximum of one region and the second deployment stage can deploy to a maximum number specified in the `regionFanoutFactor`. If you do not provide a `regionFanoutFactor`, by default the value is three. For example: If 1st deployment stage deploys to one region and 2nd deployment stage deploys to three regions, 3rd deployment stage can deploy to 12 regions, that is, sum of previous stages multiplied by the region fanout (three) number. The rule is NON\_COMPLIANT if the deployment is in more than one region in 1st stage or three regions in 2nd stage or 12 regions in 3rd stage.

**Identifier:** CODEPIPELINE\_REGION\_FANOUT\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), China (Ningxia), AWS GovCloud (US-East), AWS GovCloud (US-West), Asia Pacific (Hong Kong), Asia Pacific (Osaka), Europe (Milan), Europe (Stockholm), Middle East (Bahrain), Africa (Cape Town) Region

**Parameters:**

regionFanoutFactor (Optional), Type: int, Default: 3

The number of regions the AWS CodePipeline has deployed to in all previous stages is the acceptable number of regions any stage can deploy to.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## cw-loggroup-retention-period-check

Checks whether Amazon CloudWatch LogGroup retention period is set to specific number of days. The rule is NON\_COMPLIANT if the retention period is not set or is less than the configured retention period.

**Identifier:** CW\_LOGGROUP\_RETENTION\_PERIOD\_CHECK

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

LogGroupNames (Optional), Type: CSV

A comma-separated list of Log Group names to check the retention period.

MinRetentionTime (Optional), Type: int

Specify the retention time. Valid values are: 1, 3, 5, 7, 14, 30, 60, 90, 120, 150, 180, 365, 400, 545, 731, 1827, and 3653. The default retention period is 365 days.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## dax-encryption-enabled

Checks that Amazon DynamoDB Accelerator (DAX) clusters are encrypted. The rule is NON\_COMPLIANT if a DAX cluster is not encrypted

**Identifier:** DAX\_ENCRYPTION\_ENABLED

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), China (Ningxia), AWS GovCloud (US-East), AWS GovCloud (US-West), Asia Pacific (Hong Kong), Asia Pacific (Osaka), Asia Pacific (Seoul), Canada (Central), Europe (Milan), Europe (Stockholm), Middle East (Bahrain), Africa (Cape Town) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## db-instance-backup-enabled

Checks if RDS DB instances have backups enabled. Optionally, the rule checks the backup retention period and the backup window.

**Identifier:** DB\_INSTANCE\_BACKUP\_ENABLED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

backupRetentionPeriod (Optional), Type: int

Retention period for backups.

preferredBackupWindow (Optional), Type: String

Time range in which backups are created.

checkReadReplicas (Optional), Type: boolean

Checks whether RDS DB instances have backups enabled for read replicas.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## desired-instance-tenancy

Checks instances for specified tenancy. Specify AMI IDs to check instances that are launched from those AMIs or specify host IDs to check whether instances are launched on those Dedicated Hosts. Separate multiple ID values with commas.

**Identifier:** DESIRED\_INSTANCE\_TENANCY

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

tenancy, Type: String

Desired tenancy of the instances. Valid values are DEDICATED, HOST and DEFAULT.

imageId (Optional), Type: CSV

The rule evaluates instances launched only from AMIs with the specified IDs. Separate multiple AMI IDs with commas.

hostId (Optional), Type: CSV

The IDs of the EC2 Dedicated Hosts on which the instances are meant to be launched. Separate multiple Host IDs with commas.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## desired-instance-type

Checks instances for specified tenancy. Specify AMI IDs to check instances that are launched from those AMIs or specify host IDs to check whether instances are launched on those Dedicated Hosts. Separate multiple ID values with commas.

For a list of supported Amazon EC2 instance types, see [Instance Types](#) in the *Amazon EC2 User Guide for Linux Instances*.

**Identifier:** DESIRED\_INSTANCE\_TYPE

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

instanceType, Type: CSV

Comma-separated list of EC2 instance types (for example, "t2.small, m4.large, i2.xlarge").

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## dms-replication-not-public

Checks whether AWS Database Migration Service replication instances are public. The rule is NON\_COMPLIANT if PubliclyAccessible field is True.

**Identifier:** DMS\_REPLICATION\_NOT\_PUBLIC

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## dynamodb-autoscaling-enabled

Checks if Auto Scaling or On-Demand is enabled on your DynamoDB tables and/or global secondary indexes. Optionally you can set the read and write capacity units for the table or global secondary index.

**Identifier:** DYNAMODB\_AUTOSCALING\_ENABLED

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except AWS GovCloud (US-East), AWS GovCloud (US-West) Region

**Parameters:**

minProvisionedReadCapacity (Optional), Type: int

The minimum number of units that should be provisioned with read capacity in the Auto Scaling group.

maxProvisionedReadCapacity (Optional), Type: int

The minimum number of units that should be provisioned with write capacity in the Auto Scaling group.

targetReadUtilization (Optional), Type: double

The maximum number of units that should be provisioned with read capacity in the Auto Scaling group.

minProvisionedWriteCapacity (Optional), Type: int

The maximum number of units that should be provisioned with write capacity in the Auto Scaling group.

maxProvisionedWriteCapacity (Optional), Type: int

The target utilization percentage for read capacity. Target utilization is expressed in terms of the ratio of consumed capacity to provisioned capacity.

targetWriteUtilization (Optional), Type: double

The target utilization percentage for write capacity. Target utilization is expressed in terms of the ratio of consumed capacity to provisioned capacity.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## dynamodb-in-backup-plan

Checks whether Amazon DynamoDB table is present in AWS Backup Plans. The rule is NON\_COMPLIANT if Amazon DynamoDB tables are not present in any AWS Backup plan.

**Identifier:** DYNAMODB\_IN\_BACKUP\_PLAN

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except AWS GovCloud (US-East), AWS GovCloud (US-West), Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## dynamodb-pitr-enabled

Checks that point in time recovery (PITR) is enabled for Amazon DynamoDB tables. The rule is NON\_COMPLIANT if point in time recovery is not enabled for Amazon DynamoDB tables.

**Identifier:** DYNAMODB\_PITR\_ENABLED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## dynamodb-table-encrypted-kms

Checks if Amazon DynamoDB table is encrypted with AWS Key Management Service (KMS). The rule is NON\_COMPLIANT if Amazon DynamoDB table is not encrypted with AWS KMS. The rule is also NON\_COMPLIANT if the encrypted AWS KMS key is not present in `kmsKeyArns` input parameter.

**Identifier:** DYNAMODB\_TABLE\_ENCRYPTED\_KMS

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

`kmsKeyArns` (Optional), Type: CSV

Comma separated list of AWS KMS key ARNs allowed for encrypting Amazon DynamoDB Tables.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## dynamodb-table-encryption-enabled

Checks if the Amazon DynamoDB tables are encrypted and checks their status. The rule is COMPLIANT if the status is enabled or enabling.

**Identifier:** DYNAMODB\_TABLE\_ENCRYPTION\_ENABLED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Ningxia), Asia Pacific (Hong Kong), Asia Pacific (Osaka), Europe (Milan), Europe (Stockholm), Middle East (Bahrain), Africa (Cape Town) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## dynamodb-throughput-limit-check

Checks if provisioned DynamoDB throughput is approaching the maximum limit for your account. By default, the rule checks if provisioned throughput exceeds a threshold of 80 percent of your account limits.

**Identifier:** DYNAMODB\_THROUGHPUT\_LIMIT\_CHECK

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

accountRCUThresholdPercentage (Optional), Type: int, Default: 80

Percentage of provisioned read capacity units for your account. When this value is reached, the rule is marked as NON\_COMPLIANT.

accountWCUThresholdPercentage (Optional), Type: int, Default: 80

Percentage of provisioned write capacity units for your account. When this value is reached, the rule is marked as NON\_COMPLIANT.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## ebs-in-backup-plan

Check if Amazon Elastic Block Store (Amazon EBS) volumes are added in backup plans of AWS Backup. The rule is NON\_COMPLIANT if Amazon EBS volumes are not included in backup plans.

**Identifier:** EBS\_IN\_BACKUP\_PLAN

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except AWS GovCloud (US-East), AWS GovCloud (US-West), Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## ebs-optimized-instance

Checks whether EBS optimization is enabled for your EC2 instances that can be EBS-optimized.

**Identifier:** EBS\_OPTIMIZED\_INSTANCE

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## ebs-snapshot-public-restorable-check

Checks whether Amazon Elastic Block Store (Amazon EBS) snapshots are not publicly restorable. The rule is NON\_COMPLIANT if one or more snapshots with RestorableByUserIds field are set to all, that is, Amazon EBS snapshots are public.

**Identifier:** EBS\_SNAPSHOT\_PUBLIC\_RESTORABLE\_CHECK

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## ec2-ebs-encryption-by-default

Check that Amazon Elastic Block Store (EBS) encryption is enabled by default. The rule is NON\_COMPLIANT if the encryption is not enabled.

**Identifier:** EC2\_EBS\_ENCRYPTION\_BY\_DEFAULT

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## ec2-imdsv2-check

Checks whether your Amazon Elastic Compute Cloud (Amazon EC2) instance metadata version is configured with Instance Metadata Service Version 2 (IMDSv2). The rule is NON\_COMPLIANT if the HttpTokens is set to optional.

**Identifier:** EC2\_IMDSV2\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## ec2-instance-detailed-monitoring-enabled

Checks if detailed monitoring is enabled for EC2 instances. The rule is NON\_COMPLIANT if detailed monitoring is not enabled.

**Identifier:** EC2\_INSTANCE\_DETAILED\_MONITORING\_ENABLED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## ec2-instance-managed-by-systems-manager

Checks whether the Amazon EC2 instances in your account are managed by AWS Systems Manager.

**Note**

This rule does not consider changes in the `PingStatus` of an instance in Systems Manager, for example, `Status - Connection Lost`. The rule reports such instances as compliant.

**Identifier:** EC2\_INSTANCE\_MANAGED\_BY\_SSM

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## ec2-instance-no-public-ip

Checks whether Amazon Elastic Compute Cloud (Amazon EC2) instances have a public IP association. The rule is `NON_COMPLIANT` if the `publicIp` field is present in the Amazon EC2 instance configuration item. This rule applies only to IPv4.

**Identifier:** EC2\_INSTANCE\_NO\_PUBLIC\_IP

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## ec2-instance-profile-attached

Checks if an Amazon Elastic Compute Cloud (Amazon EC2) instance has an Identity and Access Management (IAM) profile attached to it. This rule is `NON_COMPLIANT` if no IAM profile is attached to the Amazon EC2 instance.

**Identifier:** EC2\_INSTANCE\_PROFILE\_ATTACHED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

`IamInstanceProfileArnList` (Optional), Type: CSV

Comma-separated list of IAM profile Amazon Resource Names (ARNs) that can be attached to Amazon EC2 instances.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## ec2-managedinstance-applications-blacklisted

Checks that none of the specified applications are installed on the instance. Optionally, specify the version. Newer versions will not be blacklisted. Optionally, specify the platform to apply the rule only to instances running that platform.

**Identifier:** EC2\_MANAGEDINSTANCE\_APPLICATIONS\_BLACKLISTED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

applicationNames, Type: CSV

Comma-separated list of application names. Optionally, specify versions appended with ':' (for example, 'Chrome:0.5.3, Firefox').

**Note**

The application names must be an exact match. For example, use **firefox** on Linux or **firefox-compatible** on Amazon Linux. In addition, AWS Config does not currently support wildcards for the *applicationNames* parameter (for example, **firefox\***).

platformType (Optional), Type: String

Platform type (for example, 'Linux' or 'Windows').

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## ec2-managedinstance-applications-required

Checks if all of the specified applications are installed on the instance. Optionally, specify the minimum acceptable version. You can also specify the platform to apply the rule only to instances running that platform.

**Note**

Ensure that SSM agent is running on the EC2 instance and configure SSM agents.

**Identifier:** EC2\_MANAGEDINSTANCE\_APPLICATIONS\_REQUIRED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

applicationNames, Type: CSV

Comma-separated list of application names. Optionally, specify versions appended with ':' (for example, 'Chrome:0.5.3, Firefox').

**Note**

The application names must be an exact match. For example, use **firefox** on Linux or **firefox-compat** on Amazon Linux. In addition, AWS Config does not currently support wildcards for the *applicationNames* parameter (for example, **firefox\***).

platformType (Optional), Type: String

Platform type (for example, 'Linux' or 'Windows').

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## ec2-managedinstance-association-compliance-status-check

Checks whether the compliance status of the AWS Systems Manager association compliance is COMPLIANT or NON\_COMPLIANT after the association execution on the instance. The rule is compliant if the field status is COMPLIANT.

**Identifier:** EC2\_MANAGEDINSTANCE\_ASSOCIATION\_COMPLIANCE\_STATUS\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## ec2-managedinstance-inventory-blacklisted

Checks whether instances managed by Amazon EC2 Systems Manager are configured to collect blacklisted inventory types.

**Identifier:** EC2\_MANAGEDINSTANCE\_INVENTORY\_BLACKLISTED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

inventoryNames, Type: CSV

Comma separated list of Systems Manager inventory types (for example, 'AWS:Network, AWS:WindowsUpdate').

platformType (Optional), Type: String

Platform type (for example, 'Linux').

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## ec2-managedinstance-patch-compliance-status-check

Checks whether the compliance status of the AWS Systems Manager patch compliance is COMPLIANT or NON\_COMPLIANT after the patch installation on the instance. The rule is compliant if the field status is COMPLIANT.

**Identifier:** EC2\_MANAGEDINSTANCE\_PATCH\_COMPLIANCE\_STATUS\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Osaka), Europe (Milan), Middle East (Bahrain), Africa (Cape Town) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## ec2-managedinstance-platform-check

Checks whether EC2 managed instances have the desired configurations.

**Identifier:** EC2\_MANAGEDINSTANCE\_PLATFORM\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

platformType, Type: String

Platform type (for example, 'Linux').

platformVersion (Optional), Type: String

Platform version (for example, '2016.09').

agentVersion (Optional), Type: String

Agent version (for example, '2.0.433.0').

platformName (Optional), Type: String

The version of the platform (for example, '2016.09')

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## ec2-security-group-attached-to-eni

Checks that non-default security groups are attached to Amazon Elastic Compute Cloud (EC2) instances or an elastic network interfaces (ENIs). The rule returns NON\_COMPLIANT if the security group is not associated with an EC2 instance or an ENI.

**Identifier:** EC2\_SECURITY\_GROUP\_ATTACHED\_TO\_ENI

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## ec2-stopped-instance

Checks if there are instances stopped for more than the allowed number of days. The instance is NON\_COMPLIANT if the state of the ec2 instance has been stopped for longer than the allowed number of days.

**Identifier:** EC2\_STOPPED\_INSTANCE

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

AllowedDays (Optional), Type: int, Default: 30

The number of days an ec2 instance can be stopped before it is NON\_COMPLIANT. The default number of days is 30.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## ec2-volume-inuse-check

Checks if EBS volumes are attached to EC2 instances. Optionally checks if EBS volumes are marked for deletion when an instance is terminated.

**Identifier:** EC2\_VOLUME\_INUSE\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

deleteOnTermination (Optional), Type: boolean

EBS volumes are marked for deletion when an instance is terminated. Possible values: True or False (other input values are marked as non-compliant).

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## ecs-task-definition-user-for-host-mode-check

Checks if an Amazon Elastic Container Service (Amazon ECS) task definition with host networking mode has 'privileged' or 'user' container definitions. The rule is NON\_COMPLIANT for task definitions with host network mode and container definitions of privileged=false or empty and user=root or empty.

**Identifier:** ECS\_TASK\_DEFINITION\_USER\_FOR\_HOST\_MODE\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## efs-encrypted-check

Checks if Amazon Elastic File System (Amazon EFS) is configured to encrypt the file data using AWS Key Management Service (AWS KMS). The rule is NON\_COMPLIANT if the encrypted key is set to false on `DescribeFileSystems` or if the `KmsKeyId` key on `DescribeFileSystems` does not match the `KmsKeyId` parameter.

**Identifier:** EFS\_ENCRYPTED\_CHECK

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

KmsKeyId (Optional), Type: String

Amazon Resource Name (ARN) of the KMS key that is used to encrypt the EFS file system.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## efs-in-backup-plan

Checks whether Amazon Elastic File System (Amazon EFS) file systems are added in the backup plans of AWS Backup. The rule is NON\_COMPLIANT if EFS file systems are not included in the backup plans.

**Identifier:** EFS\_IN\_BACKUP\_PLAN

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except AWS GovCloud (US-East), AWS GovCloud (US-West), Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## eip-attached

Checks if all Elastic IP addresses that are allocated to an AWS account are attached to EC2 instances or in-use elastic network interfaces (ENIs).

**Note**

Results might take up to 6 hours to become available after an evaluation occurs.

**Identifier:** EIP\_ATTACHED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## eks-endpoint-no-public-access

Checks whether Amazon Elastic Kubernetes Service (Amazon EKS) endpoint is not publicly accessible. The rule is NON\_COMPLIANT if the endpoint is publicly accessible.

**Identifier:** EKS\_ENDPOINT\_NO\_PUBLIC\_ACCESS

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except AWS GovCloud (US-East), AWS GovCloud (US-West), Asia Pacific (Osaka), Europe (Milan), US West (N. California), Africa (Cape Town) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## eks-secrets-encrypted

Checks if Amazon Elastic Kubernetes Service clusters are configured to have Kubernetes secrets encrypted using AWS Key Management Service (KMS) keys.

- This rule is COMPLIANT if an EKS cluster has an encryptionConfig with secrets as one of the resources.
- This rule is also COMPLIANT if the key used to encrypt EKS secrets matches with the parameter.
- This rule is NON\_COMPLIANT if an EKS cluster does not have an encryptionConfig or if the encryptionConfig resources do not include secrets.
- This rule is also NON\_COMPLIANT if the key used to encrypt EKS secrets does not match with the parameter.

**Identifier:** EKS\_SECRETS\_ENCRYPTED

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Osaka), Europe (Milan), US West (N. California), Africa (Cape Town) Region

**Parameters:**

kmsKeyArns (Optional), Type: CSV

Comma separated list of Amazon Resource Name (ARN) of the KMS key that should be used for encrypted secrets in an EKS cluster.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## elasticache-redis-cluster-automatic-backup-check

Check if the Amazon ElastiCache Redis clusters have automatic backup turned on. The rule is NON\_COMPLIANT if the SnapshotRetentionLimit for Redis cluster is less than the SnapshotRetentionPeriod parameter. For example: If the parameter is 15 then the rule is non-compliant if the snapshotRetentionPeriod is between 0-15.

**Identifier:** ELASTICACHE\_REDIS\_CLUSTER\_AUTOMATIC\_BACKUP\_CHECK

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

snapshotRetentionPeriod (Optional), Type: int, Default: 15

Minimum snapshot retention period in days for Redis cluster. Default is 15 days.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## elasticache-redis-cluster-auto-backup-check

The rule is NON\_COMPLIANT if SnapshotRetentionLimit for Redis cluster is 0, or less than the SnapshotRetentionPeriod parameter.

**Identifier:** ELASTICACHE\_REDIS\_CLUSTER\_AUTO\_BACKUP\_CHECK

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

snapshotRetentionPeriod (Optional), Type: int, Default: 15

Minimum snapshot retention period in days for Redis cluster. Default is 15 days.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## elasticsearch-encrypted-at-rest

Checks if Amazon Elasticsearch Service (Amazon ES) domains have encryption at rest configuration enabled. The rule is NON\_COMPLIANT if the EncryptionAtRestOptions field is not enabled.

**Identifier:** ELASTICSEARCH\_ENCRYPTED\_AT\_REST

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Ningxia) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## elasticsearch-in-vpc-only

Checks if Amazon Elasticsearch Service (Amazon ES) domains are in Amazon Virtual Private Cloud (Amazon VPC). The rule is NON\_COMPLIANT if the Amazon ES domain endpoint is public.

**Identifier:** ELASTICSEARCH\_IN\_VPC\_ONLY

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## elasticsearch-node-to-node-encryption-check

Check that Amazon ElasticSearch Service nodes are encrypted end to end. The rule is NON\_COMPLIANT if the node-to-node encryption is disabled on the domain.

**Identifier:** ELASTICSEARCH\_NODE\_TO\_NODE\_ENCRYPTION\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), China (Ningxia), Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## elastic-beanstalk-managed-updates-enabled

Checks if managed platform updates in an AWS Elastic Beanstalk environment is enabled. The rule is COMPLIANT if the value for `ManagedActionsEnabled` is set to true. The rule is NON\_COMPLIANT if the value for `ManagedActionsEnabled` is set to false, or if a parameter is provided and its value does not match the existing configurations.

**Identifier:** ELASTIC\_BEANSTALK\_MANAGED\_UPDATES\_ENABLED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

UpdateLevel (Optional), Type: String

UpdateLevel: (optional): A parameter for platform update, to check if updates level will be a 'minor' version update, or a 'patch'

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## elb-acm-certificate-required

Checks if the Classic Load Balancers use SSL certificates provided by AWS Certificate Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. This rule is only applicable to Classic Load Balancers. This rule does not check Application Load Balancers and Network Load Balancers.

**Identifier:** ELB\_ACM\_CERTIFICATE\_REQUIRED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), China (Ningxia), AWS GovCloud (US-East), Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## elb-cross-zone-load-balancing-enabled

Checks if cross-zone load balancing is enabled for the Classic Load Balancers (CLBs). This rule is NON\_COMPLIANT if cross-zone load balancing is not enabled for a CLB.

**Identifier:** ELB\_CROSS\_ZONE\_LOAD\_BALANCING\_ENABLED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## elb-custom-security-policy-ssl-check

Checks whether your Classic Load Balancer SSL listeners are using a custom policy. The rule is only applicable if there are SSL listeners for the Classic Load Balancer.

**Identifier:** ELB\_CUSTOM\_SECURITY\_POLICY\_SSL\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except AWS GovCloud (US-East), Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

sslProtocolsAndCiphers, Type: String

Comma-separated list of ciphers and protocols.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## elb-deletion-protection-enabled

Checks if Elastic Load Balancing has deletion protection enabled. The rule is NON\_COMPLIANT if `deletion_protection.enabled` is false.

**Identifier:** ELB\_DELETION\_PROTECTION\_ENABLED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## elb-logging-enabled

Checks if the Application Load Balancer and the Classic Load Balancer have logging enabled. The rule is NON\_COMPLIANT if the `access_logs.s3.enabled` is false or `access_logs.S3.bucket` is not equal to the `s3BucketName` that you provided.

**Identifier:** ELB\_LOGGING\_ENABLED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

s3BucketNames (Optional), Type: CSV

Comma-separated list of Amazon S3 bucket names for Amazon ELB to deliver the log files.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## elb-predefined-security-policy-ssl-check

Checks whether your Classic Load Balancer SSL listeners are using a predefined policy. The rule is only applicable if there are SSL listeners for the Classic Load Balancer.

**Identifier:** ELB\_PREDEFINED\_SECURITY\_POLICY\_SSL\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except AWS GovCloud (US-East), Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

predefinedPolicyName, Type: String

Name of the predefined policy.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## elb-tls-https-listeners-only

Checks if your Classic Load Balancer is configured with SSL or HTTPS listeners.

- If the Classic Load Balancer does not have a listener configured, then the rule returns NOT\_APPLICABLE.
- The rule is COMPLIANT if the Classic Load Balancer listeners are configured with SSL or HTTPS.
- The rule is NON\_COMPLIANT if a listener is not configured with SSL or HTTPS.

**Identifier:** ELB\_TLS\_HTTPS\_LISTENERS\_ONLY

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## emr-kerberos-enabled

Checks if Amazon EMR clusters have Kerberos enabled. The rule is NON\_COMPLIANT if a security configuration is not attached to the cluster or the security configuration does not satisfy the specified rule parameters.

**Identifier:** EMR\_KERBEROS\_ENABLED

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

TicketLifetimeInHours (Optional), Type: int

Period for which Kerberos ticket issued by cluster's KDC is valid.

Realm (Optional), Type: String

Kereberos realm name of the other realm in the trust relationship.

Domain (Optional), Type: String

Domain name of the other realm in the trust relationship.

AdminServer (Optional), Type: String

Fully qualified domain of the admin server in the other realm of the trust relationship.

KdcServer (Optional), Type: String

Fully qualified domain of the KDC server in the other realm of the trust relationship.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## emr-master-no-public-ip

Checks if Amazon Elastic MapReduce (EMR) clusters' master nodes have public IPs. The rule is NON\_COMPLIANT if the master node has a public IP.

**Note**

This rule checks clusters that are in RUNNING or WAITING state.

**Identifier:** EMR\_MASTER\_NO\_PUBLIC\_IP

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## encrypted-volumes

Checks if the EBS volumes that are in an attached state are encrypted. If you specify the ID of a KMS key for encryption using the kmsId parameter, the rule checks if the EBS volumes in an attached state are encrypted with that KMS key.

**Identifier:** ENCRYPTED\_VOLUMES

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

kmsId (Optional), Type: String

ID or ARN of the KMS key that is used to encrypt the volume.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## fms-security-groups-audit-policy-check

Checks if the security groups associated inScope resources are compliant with the master security groups at each rule level based on allowSecurityGroup and denySecurityGroup flag.

**Note**

Only AWS Firewall Manager can create this rule.

**Identifier:** FMS\_SECURITY\_GROUP\_AUDIT\_POLICY\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), China (Ningxia), AWS GovCloud (US-East), AWS GovCloud (US-West), Asia Pacific (Osaka) Region

**Parameters:**

masterSecurityGroupIds, Type: String

Comma-separated list of master Groups Ids. Rule will check if security groups associated in scope resource compliant with the master security groups at rule level.

inScope, Type: String

If true, the config rule owner is in AWS FMS Security Group Audit policy scope.

resourceTags, Type: String

The resource tags (EC2 Instance, Elastic Network Interface or Security Group) that the rule should be associated with. (for example, { "tagKey1" : ["tagValue1"], "tagKey2" : ["tagValue2", "tagValue3"] }

excludeResourceTags, Type: boolean

If true, exclude resources that match resourceTags.

resourceTypes, Type: String

The resource type supported by this rule. Can be EC2 Instance, Elastic Network Interface or Security Group.

fmsRemediationEnabled, Type: boolean

If true, AWS Firewall Manager will update non-compliant resources according to FMS policy. AWS Config ignores this parameter when customer creates this rule.

allowSecurityGroup, Type: boolean

If true, the rule will check to ensure that all the in-scope security groups are within (outside, if false) the reference security group's inbound/outbound rules.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## fms-security-groups-content-check

Checks if AWS Firewall Manager created security groups content is the same as the master security groups. The rule is NON\_COMPLIANT if the content does not match.

### Note

Only AWS Firewall Manager can create this rule.

**Identifier:** FMS\_SECURITY\_GROUP\_CONTENT\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), China (Ningxia), AWS GovCloud (US-East), AWS GovCloud (US-West), Asia Pacific (Osaka) Region

### Parameters:

vpcls, Type: String

Comma-separated list of VPC ids in the account.

securityGroupsIds, Type: String

Comma-separated list of security groups IDs created by AWS Firewall Manager in every VPC in the account. Sorted by VPC ids.

fmsRemediationEnabled, Type: boolean

If true, AWS Firewall Manager will update non-compliant resources according to FMS policy. AWS Config ignores this parameter when customer creates this rule.

revertManualSecurityGroupChangesFlag, Type: boolean

If true, AWS Firewall Manager will check the security groups in the securityGroupsIds parameter. masterSecurityGroupsIds (Optional), Type: String

This parameter only applies to AWS Firewall Manager admin account. Comma-separated list of master security groups id in AWS Firewall manager admin account. Rule will check if the AWS Firewall manager created security groups in the account are same as the master security groups.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## fms-security-groups-resource-association-check

Checks if Amazon EC2 or an elastic network interface is associated with AWS Firewall Manager security groups. The rule is NON\_COMPLIANT if the resources are not associated with FMS security groups.

**Note**

Only AWS Firewall Manager can create this rule.

**Identifier:** FMS\_SECURITY\_GROUP\_RESOURCE\_ASSOCIATION\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), China (Ningxia), AWS GovCloud (US-East), AWS GovCloud (US-West), Asia Pacific (Osaka) Region

**Parameters:**

vpcIds, Type: String

Comma-separated list of VPC ids in the account.

securityGroupsIds, Type: String

Comma-separated list of security groups IDs created by AWS Firewall Manager in every VPC in the account. Sorted by VPC.

resourceTags, Type: String

The resource tags (EC2 Instance or Elastic Network Interface or ALB or ELB) that the rule should be associated with. (for example, { "tagKey1" : ["tagValue1"], "tagKey2" : ["tagValue2", "tagValue3"] }

excludeResourceTags, Type: boolean

If true, exclude resources that match resourceTags.

resourceTypes, Type: String

The resource type supported by this rule. Can be EC2 Instance or Elastic Network Interface or ALB or ELB.

fmsRemediationEnabled, Type: boolean

If true, AWS Firewall Manager will update non-compliant resources according to FMS policy. AWS Config ignores this parameter when customer creates this rule.

exclusiveResourceSecurityGroupManagementFlag, Type: boolean

Only allow AWS Firewall Manager created security groups associate with resource if this flag set to true.

applyToAllEC2InstanceENIs (Optional), Type: boolean

If true, AWS Firewall Manager will enforce the policy on all ENIs on EC2 Instance. Otherwise AWS Firewall Manager enforce the policy on default ENI on EC2 Instance.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## fms-shield-resource-policy-check

Checks whether an Application Load Balancer, Amazon CloudFront distributions, Elastic Load Balancer or Elastic IP has AWS Shield protection. It also checks if they have web ACL associated for Application Load Balancer and Amazon CloudFront distributions.

**Identifier:** FMS\_SHIELD\_RESOURCE\_POLICY\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), China (Ningxia), AWS GovCloud (US-East), AWS GovCloud (US-West), Asia Pacific (Osaka) Region

**Parameters:**

webACLId, Type: String

The WebACLId of the web ACL.

resourceTypes, Type: String

The resource scope which this config rule will be applied to.

resourceTags (Optional), Type: String

The resource tags that the rule should be associated with (for example, { "tagKey1" : ["tagValue1"], "tagKey2" : ["tagValue2", "tagValue3"] }).

excludeResourceTags (Optional), Type: boolean

If true, exclude the resources that match the resourceTags. If false, include all the resources that match the resourceTags.

fmsManagedToken (Optional), Type: String

A token generated by AWS Firewall Manager when creating the rule in your account. AWS Config ignores this parameter when you create this rule.

fmsRemediationEnabled (Optional), Type: boolean

If true, AWS Firewall Manager will update NON\_COMPLIANT resources according to FMS policy. AWS Config ignores this parameter when you create this rule.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## fms-webacl-resource-policy-check

Checks if the web ACL is associated with an Application Load Balancer, API Gateway stage, or Amazon CloudFront distributions. When AWS Firewall Manager creates this rule, the FMS policy owner specifies the webACLId in the FMS policy and can optionally enable remediation.

**Identifier:** FMS\_WEBACL\_RESOURCE\_POLICY\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), China (Ningxia), AWS GovCloud (US-East), AWS GovCloud (US-West), Asia Pacific (Osaka) Region

**Parameters:**

webACLId, Type: String

The WebACLId of the web ACL.

resourceTags (Optional), Type: String

The resource tags (ApplicationLoadBalancer, ApiGatewayStage and CloudFront distributions) that the rule should be associated with. (for example, { "tagKey1" : ["tagValue1"], "tagKey2" : ["tagValue2", "tagValue3"] })

excludeResourceTags (Optional), Type: boolean

If true, exclude resources that match resourceTags.

fmsManagedToken (Optional), Type: String

A token generated by AWS Firewall Manager when creating the rule in customer account. AWS Config ignores this parameter when customer creates this rule.

fmsRemediationEnabled (Optional), Type: boolean

If true, AWS Firewall Manager will update non-compliant resources according to FMS policy. AWS Config ignores this parameter when customer creates this rule.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## fms-webacl-rulegroup-association-check

Checks if the rule groups associate with the web ACL at the correct priority. The correct priority is decided by the rank of the rule groups in the ruleGroups parameter. When AWS Firewall Manager creates this rule, it assigns the highest priority 0 followed by 1, 2, and so on. The FMS policy owner specifies the ruleGroups rank in the FMS policy and can optionally enable remediation.

**Identifier:** FMS\_WEBACL\_RULEGROUP\_ASSOCIATION\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), China (Ningxia), AWS GovCloud (US-East), AWS GovCloud (US-West), Asia Pacific (Osaka) Region

### Parameters:

ruleGroups, Type: String

Comma-separated list of RuleGroupIds and WafOverrideAction pairs. (for example, ruleGroupId-1:NONE, ruleGroupId2:COUNT)

fmsManagedToken (Optional), Type: String

A token generated by AWS Firewall Manager when creating the rule in customer account. AWS Config ignores this parameter when customer creates this rule.

fmsRemediationEnabled (Optional), Type: boolean

If true, AWS Firewall Manager will update non-compliant resources according to FMS policy. AWS Config ignores this parameter when customer creates this rule.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## guardduty-enabled-centralized

Checks if Amazon GuardDuty is enabled in your AWS account and region. If you provide an AWS account for centralization, the rule evaluates the Amazon GuardDuty results in the centralized account. The rule is COMPLIANT when Amazon GuardDuty is enabled.

**Identifier:** GUARDDUTY\_ENABLED\_CENTRALIZED

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), China (Ningxia), AWS GovCloud (US-East), Asia Pacific (Osaka), Europe (Milan), Middle East (Bahrain), Africa (Cape Town) Region

**Parameters:**

CentralMonitoringAccount (Optional), Type: String

Comma separated list of AWS Accounts (12-digit) where Amazon GuardDuty results are allowed to be centralized.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## guardduty-non-archived-findings

Checks whether Amazon GuardDuty has findings that are non archived. The rule is NON\_COMPLIANT if Amazon GuardDuty has non archived low/medium/high severity findings older than the specified number in the daysLowSev/daysMediumSev/daysHighSev parameter.

**Identifier:** GUARDDUTY\_NON\_ARCHIVED\_FINDINGS

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), China (Ningxia), AWS GovCloud (US-East), Asia Pacific (Osaka), Europe (Milan), Middle East (Bahrain), Africa (Cape Town) Region

**Parameters:**

daysLowSev (Optional), Type: int, Default: 30

The number of days Amazon GuardDuty low severity findings are allowed to stay non archived. The default is 30 days.

daysMediumSev (Optional), Type: int, Default: 7

The number of days Amazon GuardDuty medium severity findings are allowed to stay non archived. The default is 7 days.

daysHighSev (Optional), Type: int, Default: 1

The number of days Amazon GuardDuty high severity findings are allowed to stay non archived. The default is 1 day.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## iam-customer-policy-blocked-kms-actions

Checks that the managed AWS Identity and Access Management (IAM) policies that you create do not allow blocked actions on all AWS KMS keys. The rule is NON\_COMPLIANT if any blocked action is allowed on all AWS KMS keys by the managed IAM policy.

**Identifier:** IAM\_CUSTOMER\_POLICY\_BLOCKED\_KMS\_ACTIONS

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

blockedActionsPatterns, Type: CSV

Comma-separated list of blocked KMS action patterns, for example, kms:\*, kms:Decrypt, kms:ReEncrypt\*.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## iam-group-has-users-check

Checks whether IAM groups have at least one IAM user.

**Identifier:** IAM\_GROUP\_HAS\_USERS\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## iam-inline-policy-blocked-kms-actions

Checks that the inline policies attached to your IAM users, roles, and groups do not allow blocked actions on all AWS Key Management Service (KMS) keys. The rule is NON\_COMPLIANT if any blocked action is allowed on all KMS keys in an inline policy.

**Identifier:** IAM\_INLINE\_POLICY\_BLOCKED\_KMS\_ACTIONS

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

blockedActionsPatterns, Type: CSV

Comma-separated list of blocked KMS action patterns, for example, kms:\*, kms:Decrypt, kms:ReEncrypt\*.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## iam-no-inline-policy-check

Checks that inline policy feature is not in use. The rule is NON\_COMPLIANT if an AWS Identity and Access Management (IAM) user, IAM role or IAM group has any inline policy.

**Identifier:** IAM\_NO\_INLINE\_POLICY\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## iam-password-policy

Checks if the account password policy for IAM users meets the specified requirements indicated in the parameters. This rule is NON\_COMPLIANT if the account password policy does not meet the specified requirements.

### Important

The `true` and `false` values for the rule parameters are case-sensitive. If `true` is not provided in lowercase, it will be treated as `false`.

**Identifier:** IAM\_PASSWORD\_POLICY

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

RequireUppercaseCharacters (Optional), Type: boolean, Default: true

Require at least one uppercase character in password.

RequireLowercaseCharacters (Optional), Type: boolean, Default: true

Require at least one lowercase character in password.

RequireSymbols (Optional), Type: boolean, Default: true

Require at least one symbol in password.

RequireNumbers (Optional), Type: boolean, Default: true

Require at least one number in password.

MinimumPasswordLength (Optional), Type: int, Default: 14

Password minimum length.

PasswordReusePrevention (Optional), Type: int, Default: 24

Number of passwords before allowing reuse.

MaxPasswordAge (Optional), Type: int, Default: 90

Number of days before password expiration.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## iam-policy-blacklisted-check

Checks if for each IAM resource, a policy ARN in the input parameter is attached to the IAM resource. The rule is NON\_COMPLIANT if the policy ARN is attached to the IAM resource. AWS Config marks the resource as COMPLIANT if the IAM resource is part of the `exceptionList` parameter irrespective of the presence of the policy ARN.

**Identifier:** IAM\_POLICY\_BLACKLISTED\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

`policyArns`, Type: CSV, Default: `arn:aws:iam::aws:policy/AdministratorAccess`

Comma-separated list of IAM policy arns which should not be attached to any IAM entity.

`exceptionList` (Optional), Type: CSV

Comma-separated list IAM users, groups, or roles that are exempt from this rule. For example, users: `[user1;user2]`, groups:`[group1;group2]`, roles:`[role1;role2;role3]`.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## iam-policy-in-use

Checks whether the IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity.

**Identifier:** IAM\_POLICY\_IN\_USE

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

policyARN, Type: String

An IAM policy ARN to be checked.

policyUsageType (Optional), Type: String

Specify whether you expect the policy to be attached to an IAM user, group or role. Valid values are IAM\_USER, IAM\_GROUP, IAM\_ROLE, or ANY. Default value is ANY.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## iam-policy-no-statements-with-admin-access

Checks the IAM policies that you create for Allow statements that grant permissions to all actions on all resources. The rule is NON\_COMPLIANT if any policy statement includes "Effect": "Allow" with "Action": "\*" over "Resource": "\*".

The following policy is NON\_COMPLIANT:

```
"Statement": [
{
  "Sid": "VisualEditor",
  "Effect": "Allow",
  "Action": "*",
  "Resource": "*"
}
```

The following policy is COMPLIANT:

```
"Statement": [
{
  "Sid": "VisualEditor",
  "Effect": "Allow",
  "Action": "service:*",
  "Resource": "*"
}
```

This rule checks only the IAM policies that you create. It does not check IAM Managed Policies. When you enable the rule, this rule checks all of the customer managed policies in your account, and all new policies that you create.

**Identifier:** IAM\_POLICY\_NO\_STATEMENTS\_WITH\_ADMIN\_ACCESS

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## iam-role-managed-policy-check

Checks that the AWS Identity and Access Management (IAM) role is attached to all AWS managed policies specified in the list of managed policies. The rule is non-compliant if the IAM role is not attached to the AWS managed policy.

**Identifier:** IAM\_ROLE\_MANAGED\_POLICY\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

managedPolicyArns, Type: CSV

Comma-separated list of AWS managed policy ARNs.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## iam-root-access-key-check

Checks whether the root user access key is available. The rule is compliant if the user access key does not exist.

**Identifier:** IAM\_ROOT\_ACCESS\_KEY\_CHECK

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Osaka) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## iam-user-group-membership-check

Checks whether IAM users are members of at least one IAM group.

**Identifier:** IAM\_USER\_GROUP\_MEMBERSHIP\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

groupNames (Optional), Type: String

Comma-separated list of IAM groups in which IAM users must be members.

**Note**

This rule does not support group names with commas.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## iam-user-mfa-enabled

Checks whether the AWS Identity and Access Management users have multi-factor authentication (MFA) enabled.

**Identifier:** IAM\_USER\_MFA\_ENABLED

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## iam-user-no-policies-check

Checks that none of your IAM users have policies attached. IAM users must inherit permissions from IAM groups or roles. The rule is NONCOMPLIANT if there is at least one IAM user with policies attached.

**Identifier:** IAM\_USER\_NO\_POLICIES\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## iam-user-unused-credentials-check

Checks if your AWS Identity and Access Management (IAM) users have passwords or active access keys that have not been used within the specified number of days you provided.

**Note**

Re-evaluating this rule within 4 hours of the first evaluation will have no effect on the results.

**Identifier:** IAM\_USER\_UNUSED\_CREDENTIALS\_CHECK

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

maxCredentialUsageAge, Type: int, Default: 90

Maximum number of days a credential cannot be used. The default value is 90 days.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## restricted-ssh

Checks if the incoming SSH traffic for the security groups is accessible. The rule is COMPLIANT when IP addresses of the incoming SSH traffic in the security groups are restricted (CIDR other than 0.0.0.0/0). This rule applies only to IPv4.

**Identifier:** INCOMING\_SSH\_DISABLED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## ec2-instances-in-vpc

Checks if your EC2 instances belong to a virtual private cloud (VPC). Optionally, you can specify the VPC ID to associate with your instances.

**Identifier:** INSTANCES\_IN\_VPC

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

vpcId (Optional), Type: String

VPC ID that contains these EC2 instances.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## internet-gateway-authorized-vpc-only

Checks that Internet gateways (IGWs) are only attached to an authorized Amazon Virtual Private Cloud (VPCs). The rule is NON\_COMPLIANT if IGWs are not attached to an authorized VPC.

**Identifier:** INTERNET\_GATEWAY\_AUTHORIZED\_VPC\_ONLY

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

AuthorizedVpcIds (Optional), Type: String

Comma-separated list of the authorized VPC IDs with attached IGWs. If parameter is not provided all attached IGWs will be NON\_COMPLIANT.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## kms-cmk-not-scheduled-for-deletion

Checks whether customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (KMS). The rule is NON\_COMPLIANT if CMKs are scheduled for deletion.

**Identifier:** KMS\_CMK\_NOT\_SCHEDULED\_FOR\_DELETION

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Europe (Milan) Region

**Parameters:**

kmsKeyIds (Optional), Type: String

(Optional) Comma-separated list of specific customer managed key IDs not to be scheduled for deletion. If you do not specify any keys, the rule checks all the keys.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## lambda-concurrency-check

Checks whether the AWS Lambda function is configured with function-level concurrent execution limit. The rule is NON\_COMPLIANT if the Lambda function is not configured with function-level concurrent execution limit.

**Identifier:** LAMBDA\_CONCURRENCY\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Ningxia) Region

**Parameters:**

ConcurrencyLimitLow (Optional), Type: String

Minimum concurrency execution limit

ConcurrencyLimitHigh (Optional), Type: String

Maximum concurrency execution limit

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## lambda-dlq-check

Checks whether an AWS Lambda function is configured with a dead-letter queue. The rule is NON\_COMPLIANT if the Lambda function is not configured with a dead-letter queue.

**Identifier:** LAMBDA\_DLQ\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Ningxia) Region

**Parameters:**

dlqArns (Optional), Type: String

Comma-separated list of Amazon SQS and Amazon SNS ARNs that must be configured as the Lambda function dead-letter queue target.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## lambda-function-public-access-prohibited

Checks if the AWS Lambda function policy attached to the Lambda resource prohibits public access. If the Lambda function policy allows public access it is NON\_COMPLIANT.

**Identifier:** LAMBDA\_FUNCTION\_PUBLIC\_ACCESS\_PROHIBITED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Ningxia) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## lambda-function-settings-check

Checks that the AWS Lambda function settings for runtime, role, timeout, and memory size match the expected values.

**Identifier:** LAMBDA\_FUNCTION\_SETTINGS\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Ningxia) Region

**Parameters:**

runtime, Type: CSV

Comma-separated list of AWS Lambda runtime values  
role (Optional), Type: String

Name or ARN of the AWS Lambda execution role  
timeout (Optional), Type: int, Default: 3

AWS Lambda function timeout in seconds  
memorySize (Optional), Type: int, Default: 128

AWS Lambda function size in megabytes

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## lambda-inside-vpc

Checks whether an AWS Lambda function is allowed access to an Amazon Virtual Private Cloud. The rule is NON\_COMPLIANT if the Lambda function is not VPC enabled.

**Identifier:** LAMBDA\_INSIDE\_VPC

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Ningxia) Region

**Parameters:**

subnetIds (Optional), Type: String

Comma-separated list of Subnet IDs that Lambda functions can be associated with.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## mfa-enabled-for-iam-console-access

Checks whether AWS Multi-Factor Authentication (MFA) is enabled for all AWS Identity and Access Management (IAM) users that use a console password. The rule is compliant if MFA is enabled.

**Identifier:** MFA\_ENABLED\_FOR\_IAM\_CONSOLE\_ACCESS

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## multi-region-cloudtrail-enabled

Checks that there is at least one multi-region AWS CloudTrail. The rule is non-compliant if the trails do not match input parameters

**Identifier:** MULTI\_REGION\_CLOUD\_TRAIL\_ENABLED

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

s3BucketName (Optional), Type: String

Name of Amazon S3 bucket for AWS CloudTrail to deliver log files to.

snsTopicArn (Optional), Type: String

Amazon SNS topic ARN for AWS CloudTrail to use for notifications.

cloudWatchLogsLogGroupArn (Optional), Type: String

Amazon CloudWatch log group ARN for AWS CloudTrail to send data to.

includeManagementEvents (Optional), Type: boolean

Event selector to include management events for the AWS CloudTrail.

readWriteType (Optional), Type: String

Type of events to record. Valid values are ReadOnly, WriteOnly and ALL.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

### no-unrestricted-route-to-igw

Checks if there are public routes in the route table to an Internet Gateway (IGW). The rule is NON\_COMPLIANT if a route to an IGW has a destination CIDR block of '0.0.0.0/0' or ':::/0' or if a destination CIDR block does not match the rule parameter.

**Identifier:** NO\_UNRESTRICTED\_ROUTE\_TO\_IGW

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

routeTableIds (Optional), Type: CSV

Comma-separated list of route table IDs that can have routes to an Internet Gateway with a destination CIDR block of '0.0.0.0/0' or ':::/0'.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

### rds-automatic-minor-version-upgrade-enabled

Checks if Amazon Relational Database Service (RDS) database instances are configured for automatic minor version upgrades. The rule is NON\_COMPLIANT if the value of 'autoMinorVersionUpgrade' is false.

**Identifier:** RDS\_AUTOMATIC\_MINOR\_VERSION\_UPGRADE\_ENABLED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

### rds-cluster-deletion-protection-enabled

Checks if an Amazon Relational Database Service (Amazon RDS) cluster has deletion protection enabled. This rule is NON\_COMPLIANT if an RDS cluster does not have deletion protection enabled.

**Identifier:** RDS\_CLUSTER\_DELETION\_PROTECTION\_ENABLED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), China (Ningxia), Middle East (Bahrain), South America (Sao Paulo) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## rds-cluster-iam-authentication-enabled

Checks if an Amazon RDS Cluster has IAM authentication enabled. The rule is NON\_COMPLIANT if RDS Cluster doesn't have IAM authentication enabled.

**Identifier:** RDS\_CLUSTER\_IAM\_AUTHENTICATION\_ENABLED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## rds-enhanced-monitoring-enabled

Checks whether enhanced monitoring is enabled for Amazon Relational Database Service (Amazon RDS) instances.

**Identifier:** RDS\_ENHANCED\_MONITORING\_ENABLED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

monitoringInterval (Optional), Type: int

An integer value in seconds between points when enhanced monitoring metrics are collected for the database instance. The valid values are 1, 5, 10, 15, 30, and 60.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## rds-instance-deletion-protection-enabled

Checks if an Amazon Relational Database Service (Amazon RDS) instance has deletion protection enabled. This rule is NON\_COMPLIANT if an Amazon RDS instance does not have deletion protection enabled i.e `deletionProtection` is set to false.

### Warning

Some RDS DB instances within a Cluster (Aurora/DocumentDB) will show as non-compliant.

**Identifier:** RDS\_INSTANCE\_DELETION\_PROTECTION\_ENABLED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

### Parameters:

`databaseEngines` (Optional), Type: CSV

Comma-separated list of RDS database engines to include in the evaluation of the rule. For example, 'mysql, postgres, mariadb'.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## rds-instance-iam-authentication-enabled

Checks if an Amazon Relational Database Service (Amazon RDS) instance has AWS Identity and Access Management (IAM) authentication enabled. This rule is NON\_COMPLIANT if an Amazon RDS instance does not have AWS IAM authentication enabled i.e `configuration.iAMDatabaseAuthenticationEnabled` is set to false.

**Identifier:** RDS\_INSTANCE\_IAM\_AUTHENTICATION\_ENABLED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), China (Ningxia), Asia Pacific (Hong Kong), Asia Pacific (Osaka), Africa (Cape Town) Region

### Parameters:

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## rds-instance-public-access-check

Check whether the Amazon Relational Database Service instances are not publicly accessible. The rule is NON\_COMPLIANT if the `publiclyAccessible` field is true in the instance configuration item.

**Identifier:** RDS\_INSTANCE\_PUBLIC\_ACCESS\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## rds-in-backup-plan

Checks whether Amazon RDS database is present in back plans of AWS Backup. The rule is NON\_COMPLIANT if Amazon RDS databases are not included in any AWS Backup plan.

**Identifier:** RDS\_IN\_BACKUP\_PLAN

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except AWS GovCloud (US-East), AWS GovCloud (US-West), Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## rds-logging-enabled

Checks if log types exported to Amazon CloudWatch for an Amazon Relational Database Service (Amazon RDS) instance are enabled. The rule is NON\_COMPLIANT if any such log types are not enabled.

**Identifier:** RDS\_LOGGING\_ENABLED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Ningxia), Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

additionalLogs (Optional), Type: StringMap

Comma-separated list of engine names and log type names. For example, "additionalLogs": "oracle: general, slowquery ; aurora: alert, slowquery"

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## rds-multi-az-support

Checks whether high availability is enabled for your RDS DB instances.

In a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone. For more information, see [High Availability \(Multi-AZ\)](#) in the *Amazon RDS User Guide*.

**Note**

This rule does not evaluate Amazon Aurora DB and Amazon DocumentDB instances.

**Identifier:** RDS\_MULTI\_AZ\_SUPPORT

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates](#) (p. 192).

## rds-snapshots-public-prohibited

Checks if Amazon Relational Database Service (Amazon RDS) snapshots are public. The rule is NON\_COMPLIANT if any existing and new Amazon RDS snapshots are public.

**Note**

It can take up to 12 hours for compliance results to be captured.

**Identifier:** RDS\_SNAPSHOTS\_PUBLIC\_PROHIBITED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates](#) (p. 192).

## rds-snapshot-encrypted

Checks whether Amazon Relational Database Service (Amazon RDS) DB snapshots are encrypted. The rule is NON\_COMPLIANT, if the Amazon RDS DB snapshots are not encrypted.

**Identifier:** RDS\_SNAPSHOT\_ENCRYPTED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Europe (Milan) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## rds-storage-encrypted

Checks whether storage encryption is enabled for your RDS DB instances.

**Identifier:** RDS\_STORAGE\_ENCRYPTED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

kmsKeyId (Optional), Type: String

KMS key ID or ARN used to encrypt the storage.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## redshift-backup-enabled

Checks that Amazon Redshift automated snapshots are enabled for clusters. The rule is NON\_COMPLIANT if the value for `automatedSnapshotRetentionPeriod` is greater than `MaxRetentionPeriod` or less than `MinRetentionPeriod` or the value is 0.

**Identifier:** REDSHIFT\_BACKUP\_ENABLED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Ningxia), Asia Pacific (Osaka), Asia Pacific (Sydney), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

MinRetentionPeriod (Optional), Type: int

Minimum value for the retention period. Minimum value is 1.

MaxRetentionPeriod (Optional), Type: int

Maximum value for the retention period. Maximum value is 35.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## redshift-cluster-configuration-check

Checks whether Amazon Redshift clusters have the specified settings.

**Identifier:** REDSHIFT\_CLUSTER\_CONFIGURATION\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Middle East (Bahrain) Region

**Parameters:**

clusterDbEncrypted, Type: boolean, Default: true

Database encryption is enabled.

loggingEnabled, Type: boolean, Default: true

Audit logging is enabled.

nodeTypes (Optional), Type: CSV, Default: dc1.large

Specify node type.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## redshift-cluster-kms-enabled

Checks if Amazon Redshift clusters are using a specified AWS Key Management Service (AWS KMS) key for encryption. The rule is COMPLIANT if encryption is enabled and the cluster is encrypted with the key provided in the kmsKeyArn parameter. The rule is NON\_COMPLIANT if the cluster is not encrypted or encrypted with another key.

**Identifier:** REDSHIFT\_CLUSTER\_KMS\_ENABLED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

kmsKeyArns (Optional), Type: CSV

Comma-separated list of AWS KMS key Amazon Resource Names (ARNs) used in Amazon Redshift clusters for encryption.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## redshift-cluster-maintenancesettings-check

Checks whether Amazon Redshift clusters have the specified maintenance settings.

**Identifier:** REDSHIFT\_CLUSTER\_MAINTENANCESETTINGS\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Middle East (Bahrain) Region

**Parameters:**

allowVersionUpgrade, Type: boolean, Default: true

Allow version upgrade is enabled.

preferredMaintenanceWindow (Optional), Type: String

Scheduled maintenance window for clusters (for example, Mon:09:30-Mon:10:00).

automatedSnapshotRetentionPeriod (Optional), Type: int, Default: 1

Number of days to retain automated snapshots.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## redshift-cluster-public-access-check

Checks if Amazon Redshift clusters are not publicly accessible. The rule is NON\_COMPLIANT if the `publiclyAccessible` field is true in the cluster configuration item.

**Identifier:** REDSHIFT\_CLUSTER\_PUBLIC\_ACCESS\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## redshift-enhanced-vpc-routing-enabled

Checks if Amazon Redshift cluster has 'enhancedVpcRouting' enabled. The rule is NON\_COMPLIANT if 'enhancedVpcRouting' is not enabled or if the configuration.enhancedVpcRouting field is 'false'.

**Identifier:** REDSHIFT\_ENHANCED\_VPC\_ROUTING\_ENABLED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## redshift-require-tls-ssl

Checks whether Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. The rule is NON\_COMPLIANT if any Amazon Redshift cluster has parameter require\_SSL not set to true.

**Identifier:** REDSHIFT\_REQUIRE\_TLS\_SSL

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Europe (Milan) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## required-tags

Checks if your resources have the tags that you specify. For example, you can check whether your Amazon EC2 instances have the `CostCenter` tag. Separate multiple values with commas.

**Important**

The supported resource types for this rule are as follows:

- ACM::Certificate
- AutoScaling::AutoScalingGroup
- CloudFormation::Stack
- CodeBuild::Project
- DynamoDB::Table
- EC2::CustomerGateway
- EC2::Instance
- EC2::InternetGateway
- EC2::NetworkAcl
- EC2::NetworkInterface
- EC2::RouteTable
- EC2::SecurityGroup
- EC2::Subnet

- EC2::Volume
- EC2::VPC
- EC2::VPNConnection
- EC2::VPNGateway
- ElasticLoadBalancing::LoadBalancer
- ElasticLoadBalancingV2::LoadBalancer
- RDS::DBInstance
- RDS::DBSecurityGroup
- RDS::DBSnapshot
- RDS::DBSubnetGroup
- RDS::EventSubscription
- Redshift::Cluster
- Redshift::ClusterParameterGroup
- Redshift::ClusterSecurityGroup
- Redshift::ClusterSnapshot
- Redshift::ClusterSubnetGroup
- S3::Bucket

**Identifier:** REQUIRED\_TAGS

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

tag1Key, Type: String, Default: CostCenter

Key of the required tag.

tag1Value (Optional), Type: CSV

Optional value of the required tag. Separate multiple values with commas.

tag2Key (Optional), Type: String

Key of a second required tag.

tag2Value (Optional), Type: CSV

Optional value of the second required tag. Separate multiple values with commas.

tag3Key (Optional), Type: String

Key of a third required tag.

tag3Value (Optional), Type: CSV

Optional value of the third required tag. Separate multiple values with commas.

tag4Key (Optional), Type: String

Key of a fourth required tag.

tag4Value (Optional), Type: CSV

Optional value of the fourth required tag. Separate multiple values with commas.

tag5Key (Optional), Type: String

Key of a fifth required tag.

tag5Value (Optional), Type: CSV

Optional value of the fifth required tag. Separate multiple values with commas.

tag6Key (Optional), Type: String

Key of a sixth required tag.

tag6Value (Optional), Type: CSV

Optional value of the sixth required tag. Separate multiple values with commas.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## restricted-common-ports

Checks if the security groups in use do not allow unrestricted incoming TCP traffic to the specified ports. The rule is COMPLIANT when the IP addresses for inbound TCP connections are restricted to the specified ports. This rule applies only to IPv4.

**Identifier:** RESTRICTED\_INCOMING\_TRAFFIC

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

blockedPort1 (Optional), Type: int, Default: 20

Blocked TCP port number.

blockedPort2 (Optional), Type: int, Default: 21

Blocked TCP port number.

blockedPort3 (Optional), Type: int, Default: 3389

Blocked TCP port number.

blockedPort4 (Optional), Type: int, Default: 3306

Blocked TCP port number.

blockedPort5 (Optional), Type: int, Default: 4333

Blocked TCP port number.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## root-account-hardware-mfa-enabled

Checks whether your AWS account is enabled to use multi-factor authentication (MFA) hardware device to sign in with root credentials.

**Identifier:** ROOT\_ACCOUNT\_HARDWARE\_MFA\_ENABLED

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), China (Ningxia), AWS GovCloud (US-East), AWS GovCloud (US-West) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## root-account-mfa-enabled

Checks if your AWS account is enabled to use multi-factor authentication (MFA) hardware device to sign in with root credentials. The rule is NON\_COMPLIANT if any virtual MFA devices are permitted for signing in with root credentials.

**Identifier:** ROOT\_ACCOUNT\_MFA\_ENABLED

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), China (Ningxia), AWS GovCloud (US-East), AWS GovCloud (US-West) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## s3-account-level-public-access-blocks

Checks if the required public access block settings are configured from account level. The rule is only NON\_COMPLIANT when the fields set below do not match the corresponding fields in the configuration item.

**Note**

If you are using this rule, ensure that S3 Block Public Access is enabled. The rule is change-triggered, so it will not be invoked unless S3 Block Public Access is enabled. If S3 Block Public Access is not enabled the rule returns INSUFFICIENT\_DATA. This means that you still might have some public buckets. For more information about setting up S3 Block Public Access, see [Blocking public access to your Amazon S3 storage](#).

**Identifier:** S3\_ACCOUNT\_LEVEL\_PUBLIC\_ACCESS\_BLOCKS

**Trigger type:** Configuration changes (current status not checked, only evaluated when changes generate new events)

**Note**

This rule is only triggered by configuration changes for the specific region where the S3 endpoint is located. In all other regions, the rule is checked periodically. If a change was made in another region, there could be a delay before the rule returns NON\_COMPLIANT.

**AWS Region:** All supported AWS regions except Europe (Milan), Middle East (Bahrain) Region

**Parameters:**

IgnorePublicAcls (Optional), Type: String, Default: True

IgnorePublicAcls is enforced or not, default True

BlockPublicPolicy (Optional), Type: String, Default: True

BlockPublicPolicy is enforced or not, default True

BlockPublicAcls (Optional), Type: String, Default: True

BlockPublicAcls is enforced or not, default True

RestrictPublicBuckets (Optional), Type: String, Default: True

RestrictPublicBuckets is enforced or not, default True

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## s3-bucket-blacklisted-actions-prohibited

Checks if the Amazon Simple Storage Service bucket policy does not allow blacklisted bucket-level and object-level actions on resources in the bucket for principals from other AWS accounts. For example, the rule checks that the Amazon S3 bucket policy does not allow another AWS account to perform any s3:GetBucket\* actions and s3:DeleteObject on any object in the bucket. The rule is NON\_COMPLIANT if any blacklisted actions are allowed by the Amazon S3 bucket policy.

**Identifier:** S3\_BUCKET\_BLACKLISTED\_ACTIONS\_PROHIBITED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

blacklistedActionPattern, Type: CSV

Comma-separated list of blacklisted action patterns, for example, s3:GetBucket\* and s3:DeleteObject.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## s3-bucket-default-lock-enabled

Checks whether Amazon S3 bucket has lock enabled, by default. The rule is NON\_COMPLIANT if the lock is not enabled.

**Identifier:** S3\_BUCKET\_DEFAULT\_LOCK\_ENABLED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

mode (Optional), Type: String

mode: (optional): A mode parameter with valid values of GOVERNANCE or COMPLIANCE.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## s3-bucket-level-public-access-prohibited

Checks if Amazon Simple Storage Service (Amazon S3) buckets are publicly accessible. This rule is NON\_COMPLIANT if an Amazon S3 bucket is not listed in the `excludedPublicBuckets` parameter and bucket level settings are public.

**Identifier:** S3\_BUCKET\_LEVEL\_PUBLIC\_ACCESS\_PROHIBITED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

`excludedPublicBuckets` (Optional), Type: CSV

Comma-separated list of known allowed public Amazon S3 bucket names.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## s3-bucket-logging-enabled

Checks whether logging is enabled for your S3 buckets.

**Identifier:** S3\_BUCKET\_LOGGING\_ENABLED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

targetBucket (Optional), Type: String

Target S3 bucket for storing server access logs.

targetPrefix (Optional), Type: String

Prefix of the S3 bucket for storing server access logs.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## s3-bucket-policy-grantee-check

Checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or VPCs that you provide. The rule is COMPLIANT if a bucket policy is not present.

For example, if the input parameter to the rule is the list of two principals: 111122223333 and 444455556666 and the bucket policy specifies that only 111122223333 can access the bucket, then the rule is COMPLIANT. With the same input parameters: If the bucket policy specifies that 111122223333 and 444455556666 can access the bucket, it is also compliant. However, if the bucket policy specifies that 999900009999 can access the bucket, the rule is NON-COMPLIANT.

### Note

If a bucket policy contains more than one statement, each statement in the bucket policy is evaluated against this rule.

**Identifier:** S3\_BUCKET\_POLICY\_GRANTEE\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

### Parameters:

awsPrincipals (Optional), Type: CSV

Comma-separated list of principals such as IAM User ARNs, IAM Role ARNs and AWS accounts, for example 'arn:aws:iam::111122223333:user/Alice, arn:aws:iam::444455556666:role/Bob, 123456789012'.

servicePrincipals (Optional), Type: CSV

Comma-separated list of service principals, for example 'cloudtrail.amazonaws.com, lambda.amazonaws.com'.

federatedUsers (Optional), Type: CSV

Comma-separated list of identity providers for web identity federation such as Amazon Cognito and SAML identity providers. For example 'cognito-identity.amazonaws.com, arn:aws:iam::111122223333:saml-provider/my-provider'.

ipAddresses (Optional), Type: CSV

Comma-separated list of CIDR formatted IP addresses, for example '10.0.0.1, 192.168.1.0/24, 2001:db8::/32'.

vpcls (Optional), Type: CSV

Comma-separated list of Amazon Virtual Private Clouds (Amazon VPC) IDs, for example 'vpc-1234abc0, vpc-ab1234c0'.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

### s3-bucket-policy-not-more-permissive

Checks if your Amazon Simple Storage Service bucket policies do not allow other inter-account permissions than the control Amazon S3 bucket policy that you provide.

**Note**

If you provide an invalid parameter value, you will see the following error: Value for controlPolicy parameter must be an Amazon S3 bucket policy.

**Identifier:** S3\_BUCKET\_POLICY\_NOT\_MORE\_PERMISSIVE

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

controlPolicy, Type: String

Amazon S3 bucket policy that defines an upper bound on the permissions of your S3 buckets. The policy can be a maximum of 1024 characters long.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

### s3-bucket-public-read-prohibited

Checks if your Amazon S3 buckets do not allow public read access. The rule checks the Block Public Access settings, the bucket policy, and the bucket access control list (ACL).

The rule is compliant when both of the following are true:

- The Block Public Access setting restricts public policies or the bucket policy does not allow public read access.
- The Block Public Access setting restricts public ACLs or the bucket ACL does not allow public read access.

The rule is noncompliant when:

- If the Block Public Access setting does not restrict public policies, AWS Config evaluates whether the policy allows public read access. If the policy allows public read access, the rule is noncompliant.
- If the Block Public Access setting does not restrict public bucket ACLs, AWS Config evaluates whether the bucket ACL allows public read access. If the bucket ACL allows public read access, the rule is noncompliant.

**Identifier:** S3\_BUCKET\_PUBLIC\_READ\_PROHIBITED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

### s3-bucket-public-write-prohibited

Checks if your Amazon S3 buckets do not allow public write access. The rule checks the Block Public Access settings, the bucket policy, and the bucket access control list (ACL).

The rule is compliant when both of the following are true:

- The Block Public Access setting restricts public policies or the bucket policy does not allow public write access.
- The Block Public Access setting restricts public ACLs or the bucket ACL does not allow public write access.

The rule is noncompliant when:

- If the Block Public Access setting does not restrict public policies, AWS Config evaluates whether the policy allows public write access. If the policy allows public write access, the rule is noncompliant.
- If the Block Public Access setting does not restrict public bucket ACLs, AWS Config evaluates whether the bucket ACL allows public write access. If the bucket ACL allows public write access, the rule is noncompliant.

**Identifier:** S3\_BUCKET\_PUBLIC\_WRITE\_PROHIBITED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

### s3-bucket-replication-enabled

Checks whether the Amazon S3 buckets have cross-region replication enabled.

**Identifier:** S3\_BUCKET\_REPLICATION\_ENABLED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## s3-bucket-server-side-encryption-enabled

Checks that your Amazon S3 bucket either has Amazon S3 default encryption enabled or that the S3 bucket policy explicitly denies `put-object` requests without server side encryption that uses AES-256 or AWS Key Management Service.

**Identifier:** S3\_BUCKET\_SERVER\_SIDE\_ENCRYPTION\_ENABLED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## s3-bucket-ssl-requests-only

Checks if S3 buckets have policies that require requests to use Secure Socket Layer (SSL). The rule is COMPLIANT if buckets explicitly deny access to HTTP requests. The rule is NON\_COMPLIANT if bucket policies allow HTTP requests.

**Identifier:** S3\_BUCKET\_SSL\_REQUESTS\_ONLY

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## s3-bucket-versioning-enabled

Checks if versioning is enabled for your S3 buckets. Optionally, the rule checks if MFA delete is enabled for your S3 buckets.

**Identifier:** S3\_BUCKET\_VERSIONING\_ENABLED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

isMfaDeleteEnabled (Optional), Type: String

MFA delete is enabled for your S3 buckets.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## s3-default-encryption-kms

Checks whether the Amazon S3 buckets are encrypted with AWS Key Management Service(AWS KMS). The rule is NON\_COMPLIANT if the Amazon S3 bucket is not encrypted with AWS KMS key.

**Identifier:** S3\_DEFAULT\_ENCRYPTION\_KMS

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

kmsKeyArns (Optional), Type: CSV

Comma separated list of AWS KMS key ARNs allowed for encrypting Amazon S3 Buckets.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## sagemaker-endpoint-configuration-kms-key-configured

Checks whether AWS Key Management Service (KMS) key is configured for an Amazon SageMaker endpoint configuration. The rule is NON\_COMPLIANT if 'KmsKeyId' is not specified for the Amazon SageMaker endpoint configuration.

**Identifier:** SAGEMAKER\_ENDPOINT\_CONFIGURATION\_KMS\_KEY\_CONFIGURED

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), China (Ningxia), AWS GovCloud (US-East), Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

kmsKeyArns (Optional), Type: String

Comma-separated list of specific AWS KMS key ARNs allowed for an Amazon SageMaker endpoint configuration.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## sagemaker-notebook-instance-kms-key-configured

Check whether an AWS Key Management Service (KMS) key is configured for an Amazon SageMaker notebook instance. The rule is NON\_COMPLIANT if 'KmsKeyId' is not specified for the Amazon SageMaker notebook instance.

**Identifier:** SAGEMAKER\_NOTEBOOK\_INSTANCE\_KMS\_KEY\_CONFIGURED

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), China (Ningxia), AWS GovCloud (US-East), Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

kmsKeyArns (Optional), Type: String

Comma-separated list of AWS KMS key ARNs allowed for an Amazon SageMaker notebook instance.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## sagemaker-notebook-no-direct-internet-access

Checks whether direct internet access is disabled for an Amazon SageMaker notebook instance. The rule is NON\_COMPLIANT if Amazon SageMaker notebook instances are internet-enabled.

**Identifier:** SAGEMAKER\_NOTEBOOK\_NO\_DIRECT\_INTERNET\_ACCESS

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), China (Ningxia), AWS GovCloud (US-East), Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## secretsmanager-rotation-enabled-check

Checks if AWS Secrets Manager secret has rotation enabled. The rule also checks an optional `maximumAllowedRotationFrequency` parameter. If the parameter is specified, the rotation frequency of the secret is compared with the maximum allowed frequency. The rule is NON\_COMPLIANT if the

secret is not scheduled for rotation. The rule is also NON\_COMPLIANT if the rotation frequency is higher than the number specified in the maximumAllowedRotationFrequency parameter.

**Note**

Re-evaluating this rule within 4 hours of the first evaluation will have no effect on the results.

**Identifier:** SECRESMANAGER\_ROTATION\_ENABLED\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Osaka) Region

**Parameters:**

maximumAllowedRotationFrequency (Optional), Type: int

Maximum allowed rotation frequency of the secret in days.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## secretsmanager-scheduled-rotation-success-check

Checks whether AWS Secrets Manager secret rotation has rotated successfully as per the rotation schedule. The rule returns NON\_COMPLIANT if RotationOccurringAsScheduled is false.

**Note**

The rule returns NOT\_APPLICABLE for secrets without rotation.

**Identifier:** SECRESMANAGER\_SCHEDULED\_ROTATION\_SUCCESS\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Osaka) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## secretsmanager-secret-periodic-rotation

Checks if AWS Secrets Manager secrets have been rotated in the past specified number of days. The rule is NON\_COMPLIANT if a secret has not been rotated for more than 'maxDaysSinceRotation' number of days. The default value is 90 days.

**Identifier:** SECRESMANAGER\_SECRET\_PERIODIC\_ROTATION

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

maxDaysSinceRotation (Optional), Type: int

Maximum number of days in which a secret can remain unchanged. The default value is 90 days.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## secretsmanager-secret-unused

Checks if AWS Secrets Manager secrets have been accessed within a specified number of days. The rule is NON\_COMPLIANT if a secret has not been accessed in 'unusedForDays' number of days. The default value is 90 days.

**Identifier:** SECRETSMANAGER\_SECRET\_UNUSED

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

unusedForDays (Optional), Type: int

The number of days in which a secret can remain unused. The default value is 90 days.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## secretsmanager-using-cmk

Checks if all secrets in AWS Secrets Manager are encrypted using an AWS Key Management Service (AWS KMS) customer master key (CMK). This rule is COMPLIANT if a secret is encrypted using an AWS KMS CMK. This rule is NON\_COMPLIANT if a secret is encrypted using the default AWS KMS key.

**Identifier:** SECRETSMANAGER\_USING\_CMK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

kmsKeyArns (Optional), Type: CSV

Comma-separated list of KMS key Amazon Resource Names (ARNs) to check if the keys are used in the encryption.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## securityhub-enabled

Checks that AWS Security Hub is enabled for an AWS Account. The rule is NON\_COMPLIANT if AWS Security Hub is not enabled.

**Identifier:** SECURITYHUB\_ENABLED

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), China (Ningxia), Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## service-vpc-endpoint-enabled

Checks whether Service Endpoint for the service provided in rule parameter is created for each Amazon VPC. The rule returns NON\_COMPLIANT if an Amazon VPC doesn't have a VPC endpoint created for the service.

**Identifier:** SERVICE\_VPC\_ENDPOINT\_ENABLED

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

serviceName, Type: String

The short name or suffix for the service. Note: To get a list of available service names or valid suffix list, use DescribeVpcEndpointServices.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## shield-advanced-enabled-autorenew

Checks if AWS Shield Advanced is enabled in your AWS account and this subscription is set to automatically renew.

**Note**

The API endpoint of AWS Shield Advanced is only available in US East (N. Virginia) Region. This rule should only be scheduled to run in the US East (N. Virginia) Region.

**Identifier:** SHIELD\_ADVANCED\_ENABLED\_AUTORENEW

**Trigger type:** Periodic

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## shield-drt-access

Checks if the DDoS response team (DRT) can access your AWS account. The rule is NON\_COMPLIANT if AWS Shield Advanced is enabled but the role for DRT access is not configured.

**Identifier:** SHIELD\_DRT\_ACCESS

**Trigger type:** Periodic

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## sns-encrypted-kms

Checks if Amazon SNS topic is encrypted with AWS Key Management Service (AWS KMS). The rule is NON\_COMPLIANT if the Amazon SNS topic is not encrypted with AWS KMS. The rule is also NON\_COMPLIANT when encrypted KMS key is not present in `kmsKeyIds` input parameter.

**Identifier:** SNS\_ENCRYPTED\_KMS

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

`kmsKeyIds` (Optional), Type: CSV

Comma separated list of AWS KMS key ARNs allowed for encrypting Amazon SNS Topic.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## subnet-auto-assign-public-ip-disabled

Checks if Amazon Virtual Private Cloud (Amazon VPC) subnets are assigned a public IP address. The rule is COMPLIANT if Amazon VPC does not have subnets that are assigned a public IP address. The rule is NON\_COMPLIANT if Amazon VPC has subnets that are assigned a public IP address.

**Identifier:** SUBNET\_AUTO\_ASSIGN\_PUBLIC\_IP\_DISABLED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## vpc-default-security-group-closed

Checks that the default security group of any Amazon Virtual Private Cloud (VPC) does not allow inbound or outbound traffic. The rule returns NOT\_APPLICABLE if the security group is not default. The rule is NON\_COMPLIANT if the default security group has one or more inbound or outbound traffic.

**Identifier:** VPC\_DEFAULT\_SECURITY\_GROUP\_CLOSED

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## vpc-flow-logs-enabled

Checks whether Amazon Virtual Private Cloud flow logs are found and enabled for Amazon VPC.

**Identifier:** VPC\_FLOW\_LOGS\_ENABLED

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

trafficType (Optional), Type: String

TrafficType of flow logs

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

### vpc-network-acl-unused-check

Checks if there are unused network access control lists (network ACLs). The rule is COMPLIANT if each network ACL is associated with a subnet. The rule is NON\_COMPLIANT if a network ACL is not associated with a subnet.

**Identifier:** VPC\_NETWORK\_ACL\_UNUSED\_CHECK

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

### vpc-sg-open-only-to-authorized-ports

Checks whether any security groups with inbound 0.0.0.0/0 have TCP or UDP ports accessible. The rule is NON\_COMPLIANT when a security group with inbound 0.0.0.0/0 has a port accessible which is not specified in the rule parameters.

**Identifier:** VPC\_SG\_OPEN\_ONLY\_TO\_AUTHORIZED\_PORTS

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

authorizedTcpPorts (Optional), Type: String

Comma-separated list of TCP ports authorized to be open to 0.0.0.0/0. Ranges are defined by dash, for example, "443,1020-1025".

authorizedUdpPorts (Optional), Type: String

Comma-separated list of UDP ports authorized to be open to 0.0.0.0/0. Ranges are defined by dash, for example, "500,1020-1025".

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

### vpc-vpn-2-tunnels-up

Checks that both VPN tunnels provided by AWS Site-to-Site VPN are in UP status. The rule returns NON\_COMPLIANT if one or both tunnels are in DOWN status.

**Identifier:** VPC\_VPN\_2\_TUNNELS\_UP

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), China (Ningxia), Middle East (Bahrain) Region

**Parameters:**

None

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## wafv2-logging-enabled

Checks whether logging is enabled on AWS Web Application Firewall (WAFV2) regional and global web access control list (ACLs). The rule is NON\_COMPLIANT if the logging is enabled but the logging destination does not match the value of the parameter.

**Identifier:** WAFV2\_LOGGING\_ENABLED

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), China (Ningxia), AWS GovCloud (US-East), AWS GovCloud (US-West), Asia Pacific (Osaka), Europe (Milan), Africa (Cape Town) Region

**Parameters:**

KinesisFirehoseDeliveryStreamArns (Optional), Type: CSV

Comma separated list of Kinesis Firehose delivery stream ARNs

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

## waf-classic-logging-enabled

Checks if logging is enabled on AWS Web Application Firewall (WAF) classic global web ACLs. This rule is NON\_COMPLIANT for a global web ACL, if it does not have logging enabled.

**Identifier:** WAF\_CLASSIC\_LOGGING\_ENABLED

**Trigger type:** Periodic

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

KinesisFirehoseDeliveryStreamArns (Optional), Type: CSV

Comma separated list of Amazon Kinesis stream ARN for AWS WAF logs.

## AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see [Creating AWS Config Managed Rules With AWS CloudFormation Templates \(p. 192\)](#).

# Working with AWS Config Managed Rules

You can set up and activate AWS managed rules from the AWS Management Console, AWS CLI, or AWS Config API.

## Setting Up and Activating an AWS Managed Rule (Console)

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. In the AWS Management Console menu, verify that the region selector is set to a region that supports AWS Config rules. For the list of supported regions, see [AWS Config Regions and Endpoints](#) in the *Amazon Web Services General Reference*.
3. In the left navigation, choose **Rules**.
4. On the **Rules** page, choose **Add rule**.
5. On the **Rules** page, you can do the following:
  - Type in the search field to filter results by rule name, description, and label. For example, type **EC2** to return rules that evaluate EC2 resource types or type **periodic** to return rules that are triggered periodically.
  - Choose the arrow icon to see the next page of rules. Recently added rules are marked as **New**.
6. Choose a rule that you want to create.
7. On the **Configure rule** page, configure the rule by completing the following steps:
  - a. For **Name**, type a unique name for the rule.
  - b. If the trigger types for your rule include **Configuration changes**, specify one of the following options for **Scope of changes** with which AWS Config invokes your Lambda function:
    - **Resources** – When a resource that matches the specified resource type, or the type plus identifier, is created, changed, or deleted.
    - **Tags** – When a resource with the specified tag is created, changed, or deleted.
    - **All changes** – When a resource recorded by AWS Config is created, changed, or deleted.
  - c. If the trigger types for your rule include **Periodic**, specify the **Frequency** with which AWS Config invokes your Lambda function.
  - d. If your rule includes parameters in the **Rule parameters** section, you can customize the values for the provided keys. A parameter is an attribute that your resources must have before they are considered COMPLIANT with the rule.
8. Choose **Save**. Your new rule displays on the **Rules** page.

**Compliance** will display **Evaluating...** until AWS Config has evaluation results for your rule. A summary of the results appears after several minutes. You can update the results with the refresh button.

If the rule or function is not working as expected, you might see one of the following for **Compliance**:

- **No results reported** - AWS Config evaluated your resources against the rule. The rule did not apply to the AWS resources in its scope, the specified resources were deleted, or the evaluation results were deleted. To get evaluation results, update the rule, change its scope, or choose **Re-evaluate**.

This message may also appear if the rule didn't report evaluation results.

- **No resources in scope** - AWS Config cannot evaluate your recorded AWS resources against this rule because none of your resources are within the rule's scope. To get evaluation results, edit the rule and change its scope, or add resources for AWS Config to record by using the **Settings** page.
- **Evaluations failed** - For information that can help you determine the problem, choose the rule name to open its details page and see the error message.

## Activating an AWS Managed Rule (AWS CLI)

Use the `put-config-rule` command.

## Activating an AWS Managed Rule (API)

Use the `PutConfigRule` action.

# Creating AWS Config Managed Rules With AWS CloudFormation Templates

For supported AWS Config managed rules, you can use the AWS CloudFormation templates to create the rule for your account or update an existing AWS CloudFormation stack. A stack is a collection of related resources that you provision and update as a single unit. When you launch a stack with a template, the AWS Config managed rule is created for you. The templates create only the rule, and don't create additional AWS resources.

### Note

When AWS Config managed rules are updated, the templates are updated for the latest changes. To save a specific version of a template for a rule, download the template, and upload it to your S3 bucket.

For more information about working with AWS CloudFormation templates, see [Getting Started with AWS CloudFormation](#) in the *AWS CloudFormation User Guide*.

### To launch an AWS CloudFormation stack for an AWS Config managed rule

1. Go to the [CloudFormation console](#) and create a new stack.
2. For **Specify template**:
  - If you downloaded the template, choose **Upload a template file**, and then **Choose file** to upload the template.
  - You can also choose **Amazon S3 URL**, and enter the template URL `s3.amazonaws.com/aws-configservice-us-east-1/cloudformation-templates-for-managed-rules/THE_RULE_IDENTIFIER.template`.

### Note

The rule identifier should be written in ALL\_CAPS\_WITH\_UNDERSCORES. For example, `CLOUDWATCH_LOG_GROUP_ENCRYPTED` instead of `cloudwatch-log-group-encrypted`.

3. Choose **Next**.
4. For **Specify stack details**, type a stack name and enter parameter values for the AWS Config rule. For example, if you are using the `DESIRED_INSTANCE_TYPE` managed rule template, you can specify the instance type such as "m4.large".
5. Choose **Next**.

6. For **Options**, you can create tags or configure other advanced options. These are not required.
7. Choose **Next**.
8. For **Review**, verify that the template, parameters, and other options are correct.
9. Choose **Create**. The stack is created in a few minutes. You can view the created rule in the [AWS Config console](#).

You can use the templates to create a single stack for AWS Config managed rules or update an existing stack in your account. If you delete a stack, the managed rules created from that stack are also deleted. For more information, see [Working with Stacks](#) in the *AWS CloudFormation User Guide*.

## AWS Config Custom Rules

You can develop custom rules and add them to AWS Config. You associate each custom rule with an AWS Lambda function, which contains the logic that evaluates whether your AWS resources comply with the rule.

You associate this function with your rule, and the rule invokes the function either in response to configuration changes or periodically. The function then evaluates whether your resources comply with your rule, and sends its evaluation results to AWS Config.

The exercise in [Getting Started with Custom Rules for AWS Config \(p. 193\)](#) guides you through creating a custom rule for the first time. It includes an example function that you can add to AWS Lambda with no modification.

To learn how AWS Lambda functions work and how to develop them, see the [AWS Lambda Developer Guide](#).

### Topics

- [Getting Started with Custom Rules for AWS Config \(p. 193\)](#)
- [Developing a Custom Rule for AWS Config \(p. 195\)](#)
- [Example AWS Lambda Functions and Events for AWS Config Rules \(p. 199\)](#)

## Getting Started with Custom Rules for AWS Config

This procedure guides you through the process of creating a custom rule that evaluates whether each of your EC2 instances is the t2.micro type. AWS Config will run event-based evaluations for this rule, meaning it will check your instance configurations each time AWS Config detects a configuration change in an instance. AWS Config will flag t2.micro instances as compliant and all other instances as noncompliant. The compliance status will appear in the AWS Config console.

To have the best outcome with this procedure, you should have one or more EC2 instances in your AWS account. Your instances should include a combination of at least one t2.micro instance and other types.

To create this rule, first, you will create an AWS Lambda function by customizing a blueprint in the AWS Lambda console. Then, you will create a custom rule in AWS Config, and you will associate the rule with the function.

### Topics

- [Creating an AWS Lambda Function for a Custom Config Rule \(p. 194\)](#)
- [Creating a Custom Rule \(p. 194\)](#)

## Creating an AWS Lambda Function for a Custom Config Rule

1. Sign in to the AWS Management Console and open the AWS Lambda console at <https://console.aws.amazon.com/lambda/>.
2. In the AWS Management Console menu, verify that the region selector is set to a region that supports AWS Config rules. For the list of supported regions, see [AWS Config Regions and Endpoints](#) in the *Amazon Web Services General Reference*.
3. In the AWS Lambda console, choose **Create a Lambda function**.
4. On the **Select blueprint** page, for **filter**, type **config-rule-change-triggered**. Select the blueprint in the filter results.
5. On the **Configure triggers** page, choose **Next**.
6. On the **Configure function** page, complete the following steps:
  - a. For **Name**, type **InstanceTypeCheck**.
  - b. For **Runtime**, keep **Node.js**.
  - c. For **Code entry type**, keep **Edit code inline**. The Node.js code for your function is provided in the code editor. For this procedure, you do not need to change the code.
  - d. For **Handler**, keep **index.handler**.
  - e. For **Role**, choose **Create new role from template(s)**.
  - f. For **Role name**, type a name.
  - g. For **Policy templates**, choose **AWS Config Rules permission**.
  - h. On the **Configure function** page, choose **Next**.
  - i. On the **Review page**, verify the details about your function, and choose **Create function**. The AWS Lambda console displays your function.
7. To verify that your function is set up correctly, test it with the following steps:
  - a. Choose **Actions**, and then choose **Configure test event**.
  - b. In the **Input test event** window, for **Sample event template**, choose **AWS Config Change Triggered Rule**.
  - c. Choose **Save and test**. AWS Lambda tests your function with the example event. If your function is working as expected, an error message similar to the following appears under **Execution result**:

```
{
  "errorMessage": "Result Token provided is invalid",
  "errorType": "InvalidResultTokenException",
  . . .
}
```

The `InvalidResultTokenException` is expected because your function runs successfully only when it receives a *result token* from AWS Config. The result token identifies the AWS Config rule and the event that caused the evaluation, and the result token associates an evaluation with a rule. This exception indicates that your function has the permission it needs to send results to AWS Config. Otherwise, the following error message appears: `not authorized to perform: config:PutEvaluations`. If this error occurs, update the role that you assigned to your function to allow the `config:PutEvaluations` action, and test your function again.

## Creating a Custom Rule

1. Open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. In the AWS Management Console menu, verify that the region selector is set to the same region in which you created the AWS Lambda function for your custom rule.

3. On the **Rules** page, choose **Add rule**.
4. On the **Add rule** page, choose **Add custom rule**.
5. On the **Configure rule** page, complete the following steps:
  - a. For **Name**, type **InstanceTypesAreT2micro**.
  - b. For **Description**, type **Evaluates whether EC2 instances are the t2.micro type**.
  - c. For **AWS Lambda function ARN**, specify the ARN that AWS Lambda assigned to your function.

**Note**

The ARN that you specify in this step must not include the `$LATEST` qualifier. You can specify an ARN without a version qualifier or with any qualifier besides `$LATEST`. AWS Lambda supports function versioning, and each version is assigned an ARN with a qualifier. AWS Lambda uses the `$LATEST` qualifier for the latest version.

- d. For **Trigger type**, choose **Configuration changes**.
  - e. For **Scope of changes**, choose **Resources**.
  - f. For **Resources**, choose **Instance**.
  - g. In the **Rule parameters** section, you must specify the rule parameter that your AWS Lambda function evaluates and the desired value. The function for this procedure evaluates the `desiredInstanceType` parameter.
- For **Key**, type **desiredInstanceType**. For **Value**, type **t2.micro**.
6. Choose **Save**. Your new rule displays on the **Rules** page.

**Compliance** will display **Evaluating...** until AWS Config receives evaluation results from your AWS Lambda function. If the rule and the function are working as expected, a summary of the results appears after several minutes. For example, a result of **2 noncompliant resource(s)** indicates that 2 of your instances are not `t2.micro` instances, and a result of **Compliant** indicates that all instances are `t2.micro`. You can update the results with the refresh button.

If the rule or function is not working as expected, you might see one of the following for **Compliance**:

- **No results reported** - AWS Config evaluated your resources against the rule. The rule did not apply to the AWS resources in its scope, the specified resources were deleted, or the evaluation results were deleted. To get evaluation results, update the rule, change its scope, or choose **Re-evaluate**.

Verify that the scope includes **Instance** for **Resources**, and try again.

- **No resources in scope** - AWS Config cannot evaluate your recorded AWS resources against this rule because none of your resources are within the rule's scope. To get evaluation results, edit the rule and change its scope, or add resources for AWS Config to record by using the **Settings** page.

Verify that AWS Config is recording EC2 instances.

- **Evaluations failed** - For information that can help you determine the problem, choose the rule name to open its details page and see the error message.

If your rule works correctly and AWS Config provides evaluation results, you can learn which conditions affect the compliance status of your rule. You can learn which resources, if any, are noncompliant, and why. For more information, see [Viewing Configuration Compliance \(p. 98\)](#).

## Developing a Custom Rule for AWS Config

Complete the following procedure to create a custom rule. To create a custom rule, you first create an AWS Lambda function, which contains the evaluation logic for the rule. Then you associate the function with a custom rule that you create in AWS Config.

## Contents

- [Creating an AWS Lambda Function for a Custom Config Rule \(p. 196\)](#)
- [Creating a Custom Rule in AWS Config \(p. 197\)](#)
- [Evaluating Additional Resource Types \(p. 198\)](#)

## Creating an AWS Lambda Function for a Custom Config Rule

A *Lambda function* is custom code that you upload to AWS Lambda, and it is invoked by events that are published to it by an event source. If the Lambda function is associated with a Config rule, AWS Config invokes it when the rule's trigger occurs. The Lambda function then evaluates the configuration information that is sent by AWS Config, and it returns the evaluation results. For more information about Lambda functions, see [Function and Event Sources](#) in the *AWS Lambda Developer Guide*.

You can use a programming language that is supported by AWS Lambda to create a Lambda function for a custom rule. To make this task easier, you can customize an AWS Lambda blueprint or reuse a sample function from the AWS Config Rules GitHub repository.

### AWS Lambda blueprints

The AWS Lambda console provides sample functions, or *blueprints*, which you can customize by adding your own evaluation logic. When you create a function, you can choose one of the following blueprints:

- **config-rule-change-triggered** – Triggered when your AWS resource configurations change.
- **config-rule-periodic** – Triggered at a frequency that you choose (for example, every 24 hours).

### AWS Config Rules GitHub repository

A public repository of sample functions for custom rules is available on GitHub, a web-based code hosting and sharing service. The sample functions are developed and contributed by the AWS community. If you want to use a sample, you can copy its code into a new AWS Lambda function. To view the repository, see <https://github.com/aws-labs/aws-config-rules/>.

### To create the function for your custom rule

1. Sign in to the AWS Management Console and open the AWS Lambda console at <https://console.aws.amazon.com/lambda/>.
2. In the AWS Management Console menu, verify that the region selector is set to a region that supports AWS Config rules. For the list of supported regions, see [AWS Config Regions and Endpoints](#) in the *Amazon Web Services General Reference*.
3. Choose **Create a Lambda function**.
4. On the **Select blueprint** page, you can choose one of the blueprint functions for AWS Config rules as a starting point, or you can proceed without a blueprint by choosing **Skip**.
5. On the **Configure triggers** page, choose **Next**.
6. On the **Configure function** page, type a name and description.
7. For **Runtime**, choose the programming language in which your function is written.
8. For **Code entry type**, choose your preferred entry type. If you are using a blueprint, keep **Edit code inline**.
9. Provide your code using the method required by the code entry type that you selected. If you are using a blueprint, the function code is provided in the code editor, and you can customize it to include your own evaluation logic. Your code can evaluate the event data that AWS Config provides when it invokes your function:

- For functions based on the **config-rule-change-triggered** blueprint, or for functions triggered by configuration changes, the event data is the configuration item or an oversized configuration item object for the AWS resource that changed.
  - For functions based on the **config-rule-periodic** blueprint, or for functions triggered at a frequency that you choose, the event data is a JSON object that includes information about when the evaluation was triggered.
  - For both types of functions, AWS Config passes rule parameters in JSON format. You can define which rule parameters are passed when you create the custom rule in AWS Config.
  - For example events that AWS Config publishes when it invokes your function, see [Example Events for AWS Config Rules \(p. 204\)](#).
10. For **Handler**, specify the handler for your function. If you are using a blueprint, keep the default value.
  11. For **Role**, choose **Create new role from template(s)**.
  12. For **Role name**, type a name.
  13. For **Policy templates**, choose **AWS Config Rules permission**.
  14. On the **Configure function** page, choose **Next**.
  15. On the **Review page**, verify the details about your function, and choose **Create function**.

## Creating a Custom Rule in AWS Config

Use AWS Config to create a custom rule and associate the rule with a Lambda function.

### To create a custom rule

1. Open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. In the AWS Management Console menu, verify that the region selector is set to the same region in which you created the AWS Lambda function for your custom rule.
3. On the **Rules** page, choose **Add rule**.
4. On the **Add rule** page, choose **Add custom rule**.
5. On the **Configure rule** page, type a name and description.
6. For **AWS Lambda function ARN**, specify the ARN that AWS Lambda assigned to your function.

#### Note

The ARN that you specify in this step must not include the `$LATEST` qualifier. You can specify an ARN without a version qualifier or with any qualifier besides `$LATEST`. AWS Lambda supports function versioning, and each version is assigned an ARN with a qualifier. AWS Lambda uses the `$LATEST` qualifier for the latest version.

7. For **Trigger type**, choose one or both of the following:
  - **Configuration changes** – AWS Config invokes your Lambda function when it detects a configuration change.
  - **Periodic** – AWS Config invokes your Lambda function at the frequency that you choose (for example, every 24 hours).
8. If the trigger types for your rule include **Configuration changes**, specify one of the following options for **Scope of changes** with which AWS Config invokes your Lambda function:
  - **Resources** – When a resource that matches the specified resource type, or the type plus identifier, is created, changed, or deleted.
  - **Tags** – When a resource with the specified tag is created, changed, or deleted.
  - **All changes** – When a resource recorded by AWS Config is created, changed, or deleted.

9. If the trigger types for your rule include **Periodic**, specify the **Frequency** with which AWS Config invokes your Lambda function.
10. In the **Rule parameters** section, specify any rule parameters that your AWS Lambda function evaluates and the desired value.
11. Choose **Save**. Your new rule displays on the **Rules** page.

**Compliance** will display **Evaluating...** until AWS Config receives evaluation results from your AWS Lambda function. If the rule and the function are working as expected, a summary of results appears after several minutes. You can update the results with the refresh button.

If the rule or function is not working as expected, you might see one of the following for **Compliance**:

- **No results reported** - AWS Config evaluated your resources against the rule. The rule did not apply to the AWS resources in its scope, the specified resources were deleted, or the evaluation results were deleted. To get evaluation results, update the rule, change its scope, or choose **Re-evaluate**.

This message may also appear if the rule didn't report evaluation results.

- **No resources in scope** - AWS Config cannot evaluate your recorded AWS resources against this rule because none of your resources are within the rule's scope. You can choose which resources AWS Config records on the **Settings** page.
- **Evaluations failed** - For information that can help you determine the problem, choose the rule name to open its details page and see the error message.

#### Note

When you create a custom rule with the AWS Config console, the appropriate permissions are automatically created for you. If you create a custom rule with the AWS CLI, you need to give AWS Config permission to invoke your Lambda function, using the `aws lambda add-permission` command. For more information, see [Using Resource-Based Policies for AWS Lambda \(Lambda Function Policies\)](#) in the *AWS Lambda Developer Guide*.

## Evaluating Additional Resource Types

You can create custom rules to run evaluations for resource types not yet recorded by AWS Config. This is useful if you want to evaluate compliance for additional resource types that AWS Config doesn't currently record. For a list of additional resource types that you can evaluate with custom rules, see [AWS Resource Types Reference](#).

#### Note

The list in the AWS CloudFormation User Guide may contain recently added resource types that are not yet available for creating custom rules in AWS Config. AWS Config adds resource types support at regular intervals.

#### Example

1. You want to evaluate Amazon S3 Glacier vaults in your account. Amazon S3 Glacier vault resources are currently not recorded by AWS Config.
2. You create an AWS Lambda function that evaluates whether your Amazon S3 Glacier vaults comply with your account requirements.
3. You create a custom rule named **evaluate-glacier-vaults** and then assign your AWS Lambda function to the rule.
4. AWS Config invokes your Lambda function and then evaluates the Amazon S3 Glacier vaults against your rule.
5. AWS Config returns the evaluations and you can view the compliance results for your rule.

### Note

You can view the configuration details in the AWS Config timeline and look up resources in the AWS Config console for resources that AWS Config supports. If you configured AWS Config to record all resource types, newly supported resources will automatically be recorded. For more information, see [Supported Resource Types \(p. 9\)](#).

## Example AWS Lambda Functions and Events for AWS Config Rules

Each custom Config rule is associated with an AWS Lambda *function*, which is custom code that contains the evaluation logic for the rule. When the trigger for a Config rule occurs (for example, when AWS Config detects a configuration change), AWS Config invokes the rule's Lambda function by publishing an *event*, which is a JSON object that provides the configuration data that the function evaluates.

For more information about functions and events in AWS Lambda, see [Function and Event Sources](#) in the *AWS Lambda Developer Guide*.

### Topics

- [Example AWS Lambda Functions for AWS Config Rules \(Node.js\) \(p. 199\)](#)
- [Example Events for AWS Config Rules \(p. 204\)](#)

## Example AWS Lambda Functions for AWS Config Rules (Node.js)

AWS Lambda executes functions in response to events that are published by AWS services. The function for a custom Config rule receives an event that is published by AWS Config, and the function then uses data that it receives from the event and that it retrieves from the AWS Config API to evaluate the compliance of the rule. The operations in a function for a Config rule differ depending on whether it performs an evaluation that is triggered by configuration changes or triggered periodically.

For information about common patterns within AWS Lambda functions, see [Programming Model](#) in the *AWS Lambda Developer Guide*.

### Contents

- [Example Function for Evaluations Triggered by Configuration Changes \(p. 199\)](#)
- [Example Function for Periodic Evaluations \(p. 202\)](#)

## Example Function for Evaluations Triggered by Configuration Changes

AWS Config will invoke a function like the following example when it detects a configuration change for a resource that is within a custom rule's scope.

If you use the AWS Config console to create a rule that is associated with a function like this example, choose **Configuration changes** as the trigger type. If you use the AWS Config API or AWS CLI to create the rule, set the `MessageType` attribute to `ConfigurationItemChangeNotification` and `OversizedConfigurationItemChangeNotification`. These settings enable your rule to be triggered whenever AWS Config generates a configuration item or an oversized configuration item as a result of a resource change.

This example evaluates your resources and checks whether the instances match the resource type, `AWS::EC2::Instance`. The rule is triggered when AWS Config generates a configuration item or an oversized configuration item notification.

```
'use strict';
```

```
const aws = require('aws-sdk');

const config = new aws.ConfigService();

// Helper function used to validate input
function checkDefined(reference, referenceName) {
  if (!reference) {
    throw new Error(`Error: ${referenceName} is not defined`);
  }
  return reference;
}

// Check whether the message type is OversizedConfigurationItemChangeNotification,
function isOverSizedChangeNotification(messageType) {
  checkDefined(messageType, 'messageType');
  return messageType === 'OversizedConfigurationItemChangeNotification';
}

// Get the configurationItem for the resource using the getResourceConfigHistory API.
function getConfiguration(resourceType, resourceId, configurationCaptureTime, callback) {
  config.getResourceConfigHistory({ resourceType, resourceId, laterTime: new
  Date(configurationCaptureTime), limit: 1 }, (err, data) => {
    if (err) {
      callback(err, null);
    }
    const configurationItem = data.configurationItems[0];
    callback(null, configurationItem);
  });
}

// Convert the oversized configuration item from the API model to the original invocation
model.
function convertApiConfiguration(apiConfiguration) {
  apiConfiguration.awsAccountId = apiConfiguration.accountId;
  apiConfiguration.ARN = apiConfiguration.arn;
  apiConfiguration.configurationStateMd5Hash = apiConfiguration.configurationItemMD5Hash;
  apiConfiguration.configurationItemVersion = apiConfiguration.version;
  apiConfiguration.configuration = JSON.parse(apiConfiguration.configuration);
  if ({}.hasOwnProperty.call(apiConfiguration, 'relationships')) {
    for (let i = 0; i < apiConfiguration.relationships.length; i++) {
      apiConfiguration.relationships[i].name =
      apiConfiguration.relationships[i].relationshipName;
    }
  }
  return apiConfiguration;
}

// Based on the message type, get the configuration item either from the configurationItem
object in the invoking event or with the getResourceConfigHistory API in the
getConfiguration function.
function getConfigurationItem(invokingEvent, callback) {
  checkDefined(invokingEvent, 'invokingEvent');
  if (isOverSizedChangeNotification(invokingEvent.messageType)) {
    const configurationItemSummary =
    checkDefined(invokingEvent.configurationItemSummary, 'configurationItemSummary');
    getConfiguration(configurationItemSummary.resourceType,
    configurationItemSummary.resourceId,
    configurationItemSummary.configurationItemCaptureTime, (err, apiConfigurationItem) => {
      if (err) {
        callback(err);
      }
      const configurationItem = convertApiConfiguration(apiConfigurationItem);
      callback(null, configurationItem);
    });
  }
}
```

```
    } else {
      checkDefined(invokingEvent.configurationItem, 'configurationItem');
      callback(null, invokingEvent.configurationItem);
    }
  }

  // Check whether the resource has been deleted. If the resource was deleted, then the
  // evaluation returns not applicable.
  function isApplicable(configurationItem, event) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(event, 'event');
    const status = configurationItem.configurationItemStatus;
    const eventLeftScope = event.eventLeftScope;
    return (status === 'OK' || status === 'ResourceDiscovered') && eventLeftScope ===
    false;
  }

  // In this example, the resource is compliant if it is an instance and its type matches the
  // type specified as the desired type.
  // If the resource is not an instance, then this resource is not applicable.
  function evaluateChangeNotificationCompliance(configurationItem, ruleParameters) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(configurationItem.configuration, 'configurationItem.configuration');
    checkDefined(ruleParameters, 'ruleParameters');

    if (configurationItem.resourceType !== 'AWS::EC2::Instance') {
      return 'NOT_APPLICABLE';
    } else if (ruleParameters.desiredInstanceType ===
    configurationItem.configuration.instanceType) {
      return 'COMPLIANT';
    }
    return 'NON_COMPLIANT';
  }

  // Receives the event and context from AWS Lambda.
  exports.handler = (event, context, callback) => {
    checkDefined(event, 'event');
    const invokingEvent = JSON.parse(event.invokingEvent);
    const ruleParameters = JSON.parse(event.ruleParameters);
    getConfigurationItem(invokingEvent, (err, configurationItem) => {
      if (err) {
        callback(err);
      }
      let compliance = 'NOT_APPLICABLE';
      const putEvaluationsRequest = {};
      if (isApplicable(configurationItem, event)) {
        // Invoke the compliance checking function.
        compliance = evaluateChangeNotificationCompliance(configurationItem,
        ruleParameters);
      }
      // Initializes the request that contains the evaluation results.
      putEvaluationsRequest.Evaluations = [
        {
          ComplianceResourceType: configurationItem.resourceType,
          ComplianceResourceId: configurationItem.resourceId,
          ComplianceType: compliance,
          OrderingTimestamp: configurationItem.configurationItemCaptureTime,
        },
      ];
      putEvaluationsRequest.ResultToken = event.resultToken;

      // Sends the evaluation results to AWS Config.
      config.putEvaluations(putEvaluationsRequest, (error, data) => {
        if (error) {
          callback(error, null);
        } else if (data.FailedEvaluations.length > 0) {

```

```
        // Ends the function if evaluation results are not successfully reported to
AWS Config.
        callback(JSON.stringify(data), null);
    } else {
        callback(null, data);
    }
    });
});
};
```

## Function Operations

The function performs the following operations at runtime:

1. The function runs when AWS Lambda passes the event object to the handler function. AWS Lambda also passes a context object, which contains information and methods that the function can use while it runs. In this example, the function accepts the optional `callback` parameter, which it uses to return information to the caller.
2. The function checks whether the `messageType` for the event is a configuration item or an oversized configuration item, and then returns the configuration item.
3. The handler calls the `isApplicable` function to determine whether the resource was deleted.
4. The handler calls the `evaluateChangeNotificationCompliance` function and passes the `configurationItem` and `ruleParameters` objects that AWS Config published in the event.

The function first evaluates whether the resource is an EC2 instance. If the resource is not an EC2 instance, the function returns a compliance value of `NOT_APPLICABLE`.

The function then evaluates whether the `instanceType` attribute in the configuration item is equal to the `desiredInstanceType` parameter value. If the values are equal, the function returns `COMPLIANT`. If the values are not equal, the function returns `NON_COMPLIANT`.

5. The handler prepares to send the evaluation results to AWS Config by initializing the `putEvaluationsRequest` object. This object includes the `Evaluations` parameter, which identifies the compliance result, the resource type, and the ID of the resource that was evaluated. The `putEvaluationsRequest` object also includes the result token from the event, which identifies the rule and the event for AWS Config.
6. The handler sends the evaluation results to AWS Config by passing the object to the `putEvaluations` method of the `config` client.

## Example Function for Periodic Evaluations

AWS Config will invoke a function like the following example for periodic evaluations. Periodic evaluations occur at the frequency that you specify when you define the rule in AWS Config.

If you use the AWS Config console to create a rule that is associated with a function like this example, choose **Periodic** as the trigger type. If you use the AWS Config API or AWS CLI to create the rule, set the `MessageType` attribute to `ScheduledNotification`.

This example checks whether the total number of a specified resource exceeds a specified maximum.

```
var aws = require('aws-sdk'), // Loads the AWS SDK for JavaScript.
    config = new aws.ConfigService(), // Constructs a service object to use the
    aws.ConfigService class.
    COMPLIANCE_STATES = {
        COMPLIANT : 'COMPLIANT',
        NON_COMPLIANT : 'NON_COMPLIANT',
        NOT_APPLICABLE : 'NOT_APPLICABLE'
    };
```

```

// Receives the event and context from AWS Lambda.
exports.handler = function(event, context, callback) {
    // Parses the invokingEvent and ruleParameters values, which contain JSON objects
    // passed as strings.
    var invokingEvent = JSON.parse(event.invokingEvent),
        ruleParameters = JSON.parse(event.ruleParameters),
        noOfResources = 0;

    if (isScheduledNotification(invokingEvent)) {
        countResourceTypes(ruleParameters.applicableResourceType, "", noOfResources,
function(err, count) {
    if (err === null) {
        var putEvaluationsRequest;
        // Initializes the request that contains the evaluation results.
        putEvaluationsRequest = {
            Evaluations : [ {
                // Applies the evaluation result to the AWS account published in
the event.
                ComplianceResourceType : 'AWS:::Account',
                ComplianceResourceId : event.accountId,
                ComplianceType : evaluateCompliance(ruleParameters.maxCount,
count),
                OrderingTimestamp : new Date()
            } ],
            ResultToken : event.resultToken
        };
        // Sends the evaluation results to AWS Config.
        config.putEvaluations(putEvaluationsRequest, function(err, data) {
            if (err) {
                callback(err, null);
            } else {
                if (data.FailedEvaluations.length > 0) {
                    // Ends the function execution if evaluation results are not
successfully reported
                    callback(JSON.stringify(data));
                }
                callback(null, data);
            }
        });
    } else {
        callback(err, null);
    }
});
    } else {
        console.log("Invoked for a notification other than Scheduled Notification...
Ignoring.");
    }
};

// Checks whether the invoking event is ScheduledNotification.
function isScheduledNotification(invokingEvent) {
    return (invokingEvent.messageType === 'ScheduledNotification');
}

// Checks whether the compliance conditions for the rule are violated.
function evaluateCompliance(maxCount, actualCount) {
    if (actualCount > maxCount) {
        return COMPLIANCE_STATES.NON_COMPLIANT;
    } else {
        return COMPLIANCE_STATES.COMPLIANT;
    }
}

// Counts the applicable resources that belong to the AWS account.
function countResourceTypes(applicableResourceType, nextToken, count, callback) {

```



```

{"OK", "resourceId": "i-00000000", "ARN": "arn:aws:ec2:us-east-2:123456789012:instance/i-00000000", "awsRegion": "us-east-2", "availabilityZone": "us-east-2a",
"resourceType": "AWS::EC2::Instance", "tags": {"Foo": "Bar"}, "relationships":
[{"resourceId": "eipalloc-00000000", "resourceType": "AWS::EC2::EIP", "name":
"Is attached to ElasticIp"}], "configuration": {"foo": "bar"}, "messageType":
"ConfigurationItemChangeNotification"},
  "ruleParameters": {"myParameterKey": "myParameterValue"},
  "resultToken": "myResultToken",
  "eventLeftScope": false,
  "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
  "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-0123456",
  "configRuleName": "change-triggered-config-rule",
  "configRuleId": "config-rule-0123456",
  "accountId": "123456789012",
  "version": "1.0"
}

```

## Example Event for Evaluations Triggered by Oversized Configuration Changes

Some resource changes generate oversized configuration items. The following example event shows that the rule was triggered by an oversized configuration change for an EC2 instance.

```

{
  "invokingEvent": {"configurationItemSummary": {"changeType": "UPDATE",
"configurationItemVersion": "1.2", "configurationItemCaptureTime":
"2016-10-06T16:46:16.261Z", "configurationStateId": 0, "awsAccountId": "123456789012",
"configurationItemStatus": "OK", "resourceType": "AWS::EC2::Instance",
"resourceId": "i-00000000", "resourceName": null, "ARN": "arn:aws:ec2:us-
west-2:123456789012:instance/i-00000000", "awsRegion": "us-west-2", "availabilityZone":
"us-west-2a", "configurationStateMd5Hash": "8f1ee69b287895a0f8bc5753eca68e96",
"resourceCreationTime": "2016-10-06T16:46:10.489Z"}, "messageType":
"OversizedConfigurationItemChangeNotification"},
  "ruleParameters": {"myParameterKey": "myParameterValue"},
  "resultToken": "myResultToken",
  "eventLeftScope": false,
  "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
  "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-rule-
ec2-managed-instance-inventory",
  "configRuleName": "change-triggered-config-rule",
  "configRuleId": "config-rule-0123456",
  "accountId": "123456789012",
  "version": "1.0"
}

```

## Example Event for Evaluations Triggered by Periodic Frequency

AWS Config publishes an event when it evaluates your resources at a frequency that you specify (such as every 24 hours). The following example event shows that the rule was triggered by a periodic frequency.

```

{
  "invokingEvent": {"awsAccountId": "123456789012", "notificationCreationTime":
"2016-07-13T21:50:00.373Z", "messageType": "ScheduledNotification", "recordVersion":
"1.0"},
  "ruleParameters": {"myParameterKey": "myParameterValue"},
  "resultToken": "myResultToken",
  "eventLeftScope": false,
  "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
  "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-0123456",
  "configRuleName": "periodic-config-rule",
  "configRuleId": "config-rule-6543210",
}

```

```
"accountId": "123456789012",  
"version": "1.0"  
}
```

## Event Attributes

The JSON object for an AWS Config event contains the following attributes:

### `invokingEvent`

The event that triggers the evaluation for a rule. If the event is published in response to a resource configuration change, the value for this attribute is a string that contains a JSON `configurationItem` or a `configurationItemSummary` (for oversized configuration items). The configuration item represents the state of the resource at the moment that AWS Config detected the change. For an example of a configuration item, see the output produced by the `get-resource-config-history` AWS CLI command in [Viewing Configuration History \(p. 45\)](#).

If the event is published for a periodic evaluation, the value is a string that contains a JSON object. The object includes information about the evaluation that was triggered.

For each type of event, a function must parse the string with a JSON parser to be able to evaluate its contents, as shown in the following Node.js example:

```
var invokingEvent = JSON.parse(event.invokingEvent);
```

### `ruleParameters`

Key/value pairs that the function processes as part of its evaluation logic. You define parameters when you use the AWS Config console to create a custom rule. You can also define parameters with the `InputParameters` attribute in the `PutConfigRule` AWS Config API request or the `put-config-rule` AWS CLI command.

The JSON code for the parameters is contained within a string, so a function must parse the string with a JSON parser to be able to evaluate its contents, as shown in the following Node.js example:

```
var ruleParameters = JSON.parse(event.ruleParameters);
```

### `resultToken`

A token that the function must pass to AWS Config with the `PutEvaluations` call.

### `eventLeftScope`

A Boolean value that indicates whether the AWS resource to be evaluated has been removed from the rule's scope. If the value is `true`, the function indicates that the evaluation can be ignored by passing `NOT_APPLICABLE` as the value for the `ComplianceType` attribute in the `PutEvaluations` call.

### `executionRoleArn`

The ARN of the IAM role that is assigned to AWS Config.

### `configRuleArn`

The ARN that AWS Config assigned to the rule.

### `configRuleName`

The name that you assigned to the rule that caused AWS Config to publish the event and invoke the function.

`configRuleId`

The ID that AWS Config assigned to the rule.

`accountId`

The ID of the AWS account that owns the rule.

`version`

A version number assigned by AWS. The version will increment if AWS adds attributes to AWS Config events. If a function requires an attribute that is only in events that match or exceed a specific version, then that function can check the value of this attribute.

The current version for AWS Config events is 1.0.

## Managing your AWS Config Rules

You can use the AWS Config console, AWS CLI, and AWS Config API to view, add, and delete your rules.

### Contents

- [Add, View, Update and Delete Rules \(Console\) \(p. 207\)](#)
- [View, Update, and Delete Rules \(AWS CLI\) \(p. 208\)](#)
- [View, Update, and Delete Rules \(API\) \(p. 210\)](#)

## Add, View, Update and Delete Rules (Console)

On the **Rules** page, you can view the rules for the region in your account. You can also see the evaluation status for each rule.

### To view your rules

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. In the AWS Management Console, verify that the region selector is set to a region that supports AWS Config rules. For the list of supported regions, see [AWS Config Regions and Endpoints](#) in the *Amazon Web Services General Reference*.
3. Choose **Rules**. The **Rules** page shows all the rule that are currently in your AWS account. It lists the name, associated remediation action, and compliance status of each rule.
  - Choose **Add rule** to get started with creating a rule.
  - Choose a rule to see its settings, or choose a rule and **View details**.
  - See the compliance status of the rule when it evaluates your resources.
  - Choose a rule and **Edit rule** to change the configuration settings of the rule and set a remediation action for a noncompliant rule.

### To update a rule

1. Choose a rule and **Edit rule** for the rule that you want to update.
2. Modify the settings on the **Config rule** page to change your rule as needed.
3. Choose **Save**.

### To delete a rule

1. Choose a rule and **Edit rule** for the rule that you want to delete.
2. On the **Configure rule** page, choose **Delete rule**.
3. When prompted, choose **Delete**.

### To add a rule

If you choose **Add rule**, you can see the available AWS managed rules on the **Add rule** page. You can also create your own custom rule.

1. If you want to create your own rule, choose **Add custom rule** and follow the procedure in [Developing a Custom Rule for AWS Config \(p. 195\)](#).
2. To add a managed rule, choose a rule on the page and follow the procedure in [Working with AWS Config Managed Rules \(p. 191\)](#).

On the **Add rule** page, you can do the following:

- Choose **Add custom rule** to create your own rule.
- Type in the search field to filter results by rule name, description, or label. For example, type **EC2** to return rules that evaluate EC2 resource types or type **periodic** to return rules with periodic triggers. Type "new" to search for newly added rules. For more information about trigger types, see [Specifying Triggers for AWS Config Rules \(p. 101\)](#).
- Reorder the results alphabetically by choosing the arrow by the **Name** label.
- Choose the arrow icon to see the next page of rules.
- See recently added rules that are marked as **New**.
- See labels to identify the resource type that the rule evaluates and if the rule has a periodic trigger.

## View, Update, and Delete Rules (AWS CLI)

### To view your rules

- Use the `describe-config-rules` command:

```
$ aws configservice describe-config-rules
```

AWS Config returns the details for all of your rules.

### To update a rule

1. Use the `put-config-rule` command with the `--generate-cli-skeleton` parameter to create a local JSON file that has the parameters for your rule:

```
$ aws configservice put-config-rule --generate-cli-skeleton > putConfigRule.json
```

2. Open the JSON file in a text editor and remove any parameters that don't need updating, with the following exceptions:
  - Include at least one of the following parameters to identify the rule:  
ConfigRuleName, ConfigRuleArn, or ConfigRuleId.
  - If you are updating a custom rule, you must include the `Source` object and its parameters.

3. Fill in the values for the parameters that remain. To reference the details of your rule, use the **describe-config-rules** command.

For example, the following JSON code updates the resource types that are in the scope of a custom rule:

```
{
  "ConfigRule": {
    "ConfigRuleName": "ConfigRuleName",
    "Scope": {
      "ComplianceResourceTypes": [
        "AWS::EC2::Instance",
        "AWS::EC2::Volume",
        "AWS::EC2::VPC"
      ]
    },
    "Source": {
      "Owner": "CUSTOM_LAMBDA",
      "SourceIdentifier": "arn:aws:lambda:us-east-2:123456789012:function:ConfigRuleName",
      "SourceDetails": [
        {
          "EventSource": "aws.config",
          "MessageType": "ConfigurationItemChangeNotification"
        }
      ]
    }
  }
}
```

4. Use the **put-config-rule** command with the `--cli-input-json` parameter to pass your JSON configuration to AWS Config:

```
$ aws configservice put-config-rule --cli-input-json file://putConfigRule.json
```

5. To verify that you successfully updated your rule, use the **describe-config-rules** command to view the rule's configuration:

```
$ aws configservice describe-config-rules --config-rule-name ConfigRuleName
{
  "ConfigRules": [
    {
      "ConfigRuleState": "ACTIVE",
      "ConfigRuleName": "ConfigRuleName",
      "ConfigRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-rule-nnnnnn",
      "Source": {
        "Owner": "CUSTOM_LAMBDA",
        "SourceIdentifier": "arn:aws:lambda:us-east-2:123456789012:function:ConfigRuleName",
        "SourceDetails": [
          {
            "EventSource": "aws.config",
            "MessageType": "ConfigurationItemChangeNotification"
          }
        ]
      },
      "Scope": {
        "ComplianceResourceTypes": [
          "AWS::EC2::Instance",
          "AWS::EC2::Volume",
          "AWS::EC2::VPC"
        ]
      }
    }
  ]
}
```

```
    },  
    "ConfigRuleId": "config-rule-nnnnnn"  
  }  
]  
}
```

### To delete a rule

- Use the `delete-config-rule` command as shown in the following example:

```
$ aws configservice delete-config-rule --config-rule-name ConfigRuleName
```

## View, Update, and Delete Rules (API)

### To view your rules

Use the [DescribeConfigRules](#) action.

### To update or add a rule

Use the [PutConfigRule](#) action.

### To delete a rule

Use the [DeleteConfigRule](#) action.

#### Note

If a rule is creating invalid evaluation results, you might want to delete these results before you fix the rule and run a new evaluation. For more information, see [Deleting Evaluation Results](#) (p. 211).

## Evaluating Your Resources

When you create custom rules or use managed rules, AWS Config evaluates your resources against those rules. You can run on-demand evaluations for resources against your rules. For example, this is helpful when you create a custom rule and want to verify that AWS Config is correctly evaluating your resources or to identify if there is an issue with the evaluation logic of your AWS Lambda function.

### Example

1. You create a custom rule that evaluates whether your IAM users have active access keys.
2. AWS Config evaluates the resources against your custom rule.
3. An IAM user who doesn't have an active access key exists in your account. Your rule doesn't correctly flag this resource as noncompliant.
4. You fix the rule and start the evaluation again.
5. Because you fixed your rule, the rule correctly evaluates your resources, and flags the IAM user resource as noncompliant.

## Evaluating your Resources (Console)

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.

2. In the AWS Management Console menu, verify that the region selector is set to a region that supports AWS Config rules. For the list of supported regions, see [AWS Config Regions and Endpoints](#) in the *Amazon Web Services General Reference*.
3. In the navigation pane, choose **Rules**. The **Rules** page shows your rules and the compliance status for each.
4. Choose a rule from the list.
5. In the **Re-evaluate rule** section, choose **Re-evaluate**.
6. AWS Config starts evaluating the resources against your rule.

#### Note

You can re-evaluate a rule once per minute. You must wait for AWS Config to complete the evaluation for your rule before you start another evaluation. You can't run an evaluation if at the same time the rule is being updated or if the rule is being deleted.

## Evaluating your Resources (CLI)

- Use the **start-config-rules-evaluation** command.

```
$ aws configservice start-config-rules-evaluation --config-rule-names ConfigRuleName
```

AWS Config starts evaluating the recorded resource configurations against your rule.

You can also specify multiple rules in your request.

```
aws configservice start-config-rules-evaluation --config-rule-  
names ConfigRuleName1 ConfigRuleName2 ConfigRuleName3
```

## Evaluating your Resources (API)

Use the [StartConfigRulesEvaluation](#) action.

## Deleting Evaluation Results

After AWS Config evaluates your rule, you can see the evaluation results on the **Rules** page or the **Rules details** page for the rule. If the evaluation results are incorrect or if you want to evaluate again, you can delete the current evaluation results for the rule. For example, if your rule was incorrectly evaluating your resources or you recently deleted resources from your account, you can delete the evaluation results and then run a new evaluation.

## Deleting Evaluating Results (Console)

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. In the AWS Management Console menu, verify that the region selector is set to a region that supports AWS Config rules. For the list of supported regions, see [AWS Config Regions and Endpoints](#) in the *Amazon Web Services General Reference*.
3. In the navigation pane, choose **Rules**. The **Rules** page shows your rules and the compliance status.
4. Choose a rule from the list.

5. In the **Delete evaluation results** section, choose **Delete results**. AWS Config deletes the evaluation results for this rule.
6. When prompted, choose **Delete**. Deleted evaluations can't be retrieved.
7. After the evaluation results are deleted, you can manually start a new evaluation.

## Deleting Evaluating Results (CLI)

- Use the `delete-evaluation-results` command:

```
$ aws configservice delete-evaluation-results --config-rule-name ConfigRuleName
```

AWS Config deletes the evaluation results for the rule.

## Deleting Evaluating Results (API)

Use the `DeleteEvaluationResults` action.

# Enabling AWS Config Rules Across all Accounts in Your Organization

AWS Config allows you to manage AWS Config rules across all AWS accounts within an organization. You can:

- Centrally create, update, and delete AWS Config rules across all accounts in your organization.
- Deploy a common set of AWS Config rules across all accounts and specify accounts where AWS Config rules should not be created.
- Use the APIs from the master account in AWS Organizations to enforce governance by ensuring that the underlying AWS Config rules are not modifiable by your organization's member accounts.

### Note

*For deployments accross different regions*

The API call to deploy rules and conformance packs across accounts is region specific. At the organization level, you need to change the context of your API call to a different region if you want to deploy rules in other regions. For example, to deploy a rule in US East (N. Virginia), change the region to US East (N. Virginia) and then call `PutOrganizationConfigRule`.

*For accounts within an organization*

If a new account joins an organization, the rule is deployed to that account. When an account leaves an organization, the rule is removed.

Ensure AWS Config recording is on before you use the following APIs to manage AWS Config rules across all AWS accounts within an organization:

- `PutOrganizationConfigRule`, adds or updates organization config rule for your entire organization evaluating whether your AWS resources comply with your desired configurations.
- `PutOrganizationConformancePack`, deploys conformance packs across member accounts in an AWS Organization.
- `DescribeOrganizationConfigRules`, returns a list of organization config rules.
- `GetOrganizationConfigRuleDetailedStatus`, returns detailed status for each member account within an organization for a given organization config rule.

- [DescribeOrganizationConfigRuleStatuses](#), provides organization config rule deployment status for an organization.
- [DeleteOrganizationConfigRule](#), deletes the specified organization config rule and all of its evaluation results from all member accounts in that organization.

## Remediating Noncompliant AWS Resources by AWS Config Rules

AWS Config allows you to remediate noncompliant resources that are evaluated by AWS Config Rules. AWS Config applies remediation using [AWS Systems Manager Automation documents](#). These documents define the actions to be performed on noncompliant AWS resources evaluated by AWS Config Rules. You can associate SSM documents by using the AWS Management Console or by using APIs.

AWS Config provides a set of managed automation documents with remediation actions. You can also create and associate custom automation documents with AWS Config rules.

To apply remediation on noncompliant resources, you can either choose the remediation action you want to associate from a prepopulated list or create your own custom remediation actions using SSM documents. AWS Config provides a recommended list of remediation action in the AWS Management Console.

In the AWS Management Console, you can either choose to **manually** or **automatically** remediate noncompliant resources by associating remediation actions with AWS Config rules. With all remediation actions, you can either choose manual or automatic remediation.

### Topics

- [Prerequisite](#) (p. 213)
- [Setting Up Manual Remediation \(Console\)](#) (p. 213)
- [Setting Up Auto Remediation \(Console\)](#) (p. 214)
- [Setting Up and Applying a Remediation Action Remediation Using Rules and Resources \(Console\)](#) (p. 214)
- [Delete Remediation Action \(Console\)](#) (p. 216)
- [Managing Remediation \(API\)](#) (p. 217)

## Prerequisite

Before you begin to apply remediation on noncompliant resources, you must select a rule and set up remediation (manual or auto) for the rule.

## Setting Up Manual Remediation (Console)

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. Choose **Rules** on the left and then on the **Rules** page, choose **Add Rule** to add new rules to the rule list.

For existing rules, select the noncompliant rule from the rule list and choose the **Actions** dropdown list.

3. From the **Actions** dropdown list, choose **Manage remediation**. Select "Manual remediation" and then choose the appropriate remediation action from the recommended list.

Depending on the selected remediation action, you see specific parameters or no parameters.

4. (Optional): If you want to pass the resource ID of noncompliant resources to the remediation action, choose **Resource ID parameter**. If selected, at runtime that parameter is substituted with the ID of the resource to be remediated.

Each parameter has either a static value or a dynamic value. If you do not choose a specific resource ID parameter from the drop-down list, you can enter values for each key. If you choose a resource ID parameter from the drop-down list, you can enter values for all the other keys except the selected resource ID parameter.

5. Choose **Save**. The **Rules** page is displayed.

## Setting Up Auto Remediation (Console)

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. Choose **Rules** on the left and then on the **Rules** page, choose **Add Rule** to add new rules to the rule list.

For existing rules, select the noncompliant rule from the rule list and choose the **Actions** dropdown list.

3. From the **Actions** dropdown list, choose **Manage remediation**. Select "Automatic remediation" and then choose the appropriate remediation action from the recommended list.

Depending on the selected remediation action, you see specific parameters or no parameters.

4. Choose **Auto remediation** to automatically remediate noncompliant resources.

If a resource is still non-compliant after auto remediation, you can set the rule to try auto remediation again. Enter the desired retries and seconds.

### Note

There are costs associated with running a remediation script multiple times.

5. (Optional): If you want to pass the resource ID of noncompliant resources to the remediation action, choose **Resource ID parameter**. If selected, at runtime that parameter is substituted with the ID of the resource to be remediated.

Each parameter has either a static value or a dynamic value. If you do not choose a specific resource ID parameter from the drop-down list, you can enter values for each key. If you choose a resource ID parameter from the drop-down list, you can enter values for all the other keys except the selected resource ID parameter.

6. Choose **Save**. The **Rules** page is displayed.

## Setting Up and Applying a Remediation Action Remediation Using Rules and Resources (Console)

You can also set up remediation from the Rules and the Resources pages. The following procedures provide more details about each workflow.

### Using Rules

You can apply a remediation action to a noncompliant rule from **Rules** on the left.

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.

2. Choose **Rules** on the left and then on the **Rules** page, choose **Add Rule** to add new rules to the rule list.

For existing rules, select the noncompliant rule from the rule list and choose **Edit**.

3. Choose **Manage remediation** and on the **Manage remediation: *name of the rule*** page, select the appropriate remediation action from the recommended list. The remediation actions are related to AWS Systems Manager automation documents.

Depending on the selected remediation action, you will see either specific parameters or no parameters.

4. If you want to pass the resource ID of noncompliant resources to the remediation action, choose **Resource ID parameter**. If selected, at runtime that parameter is substituted with the ID of the resource to be remediated.

Each parameter has either a static value or a dynamic value. If you do not choose a specific resource ID parameter from the drop-down list, you can enter values for each key. If you choose a resource ID parameter from the drop-down list, you can enter values for all the other keys except the selected resource ID parameter.

5. Choose **Save**.
6. In the **Choose resources in scope** section, choose all the noncompliant resources. The resources in scope include those resources where this rule is applied and their compliance status.

For more information about a resource, choose **Resource actions** and either choose **View details**, **Configuration timeline**, or **Compliance timeline**.

7. Choose **Remediate**.

If the resources are remediated, the resource compliance status is compliant. To view the compliant resources, select **Compliant** from the compliance status list.

If the resources are not remediated, the action status column displays **Action execution failed (details)**. Choose **(details)** to view the main action steps invoked during the execution of the remediation action and the status of each action step.

#### Note

For troubleshooting failed remediation actions, you can run the AWS Command Line Interface (AWS CLI) command `describe-remediation-execution-status` to get detailed view of a Remediation Execution for a set of resources. The details include state, timestamps for remediation execution steps, and any error messages for the failed steps.

## Using Resources

You can also apply a remediation action to a noncompliant rule from **Resources** on the left.

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. Choose **Resources** on the left and then on the **Resource inventory** page, **Resources** is selected by default.
3. Select one or more resources from the resource type and choose **Look up**.
4. Choose the name of the appropriate noncompliant resource from the resource table.
5. On the **Resource details: *name of the resource*** page, choose one or more noncompliant rules from the rules in scope.
6. Choose **Rule actions** and select **Manage remediation**.
7. On the **Manage remediation: *name of the rule*** page, select the appropriate remediation action.

Depending on the selected remediation action, you will see either specific parameters or no parameters.

8. If you want to pass the resource ID of noncompliant resources to the remediation action, choose **Resource ID parameter**. If selected, at runtime that parameter is substituted with the ID of the resource to be remediated.

Each parameter has either a static value or a dynamic value. If you do not choose a specific resource ID parameter from the drop-down list, you can enter values for each key. If you choose a resource ID parameter from the drop-down list, you can enter values for all the other keys except the selected resource ID parameter.

9. Choose **Save**.
10. In the **Choose resources in scope** section, choose all the noncompliant resources. The resources in scope include those resources where this rule is applied and their compliance status.

For more information about a resource, choose **Resource actions** and either choose **View details**, **Configuration timeline**, or **Compliance timeline**.

11. Choose **Remediate**.

If the resources are remediated, the resource compliance status is **compliant**. To view the compliant resources, select **Compliant** from the compliance status list.

If the resources are not remediated, the action status column displays **Action execution failed (details)**. Choose **(details)** to view the main action steps invoked during the execution of the remediation action and the status of each action step.

**Note**

For troubleshooting failed remediation actions, you can run the AWS Command Line Interface (AWS CLI) command `describe-remediation-execution-status` to get detailed view of a Remediation Execution for a set of resources. The details include state, timestamps for remediation execution steps, and any error messages for the failed steps.

## Delete Remediation Action (Console)

To delete a rule first you must delete remediation action associated with that rule.

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. Choose **Rules** on the left and then on the **Rules** page, select the rule from the rule list and choose **Edit**.
3. On the rule page, choose **Edit** again.
4. On the **Edit *name of the rule*** page, in the **Choose remediation action** section, choose **Delete remediation action** and confirm your delete action.

**Note**

If remediation is in progress, the remediation action is not deleted. If you choose **Delete remediation action**, you cannot retrieve the remediation action. When you delete a remediation action, AWS Config does not delete a rule.

If the remediation action is deleted, the **Resource ID parameter** is empty and displays N/A. On the **Rules** page, the remediation action column displays **Not set** for the corresponding rule.

## Managing Remediation (API)

### Manual Remediation

Use the following AWS Config API actions to manage remediation:

- [DeleteRemediationConfiguration](#)
- [DescribeRemediationConfigurations](#)
- [DescribeRemediationExecutionStatus](#)
- [PutRemediationConfigurations](#)
- [StartRemediationExecution](#)

### Auto Remediation

Use the following AWS Config API actions to manage auto remediation:

- [PutRemediationExceptions](#)
- [DescribeRemediationExceptions](#)
- [DeleteRemediationExceptions](#)

## Tagging Your AWS Config Resources

A tag is a label that you assign to an AWS resource. Each tag consists of a *key* and an optional *value*, both of which you define. Tags make it easier to manage, search for, and filter resources.

Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type—you can quickly identify a specific resource based on the tags you've assigned to it. You can assign one or more tags to your AWS resources. Each tag has an associated value.

We recommend that you devise a set of tag keys that meets your needs for each resource type. Using a consistent set of tag keys makes it easier for you to manage your AWS resources. You can search and filter the resources based on the tags you add.

Tags are interpreted strictly as a string of characters and are not automatically assigned to your resources. You can edit tag keys and values, and you can remove tags from a resource at any time. You can set the value of a tag to an empty string, but you can't set the value of a tag to null. If you add a tag that has the same key as an existing tag on that resource, the new value overwrites the old value. If you delete a resource, any tags for the resource are also deleted.

You can work with tags using the AWS Command Line Interface (AWS CLI) and the AWS Config API reference.

### Restrictions Related to Tagging

The following basic restrictions apply to tags.

Restriction	Description
Maximum number of tags per resource	50

Restriction	Description
Maximum key length	128 Unicode characters in UTF-8
Maximum value length	256 Unicode characters in UTF-8
Prefix restriction	Do not use the <code>aws :</code> prefix in your tag names or values because it is reserved for AWS use. You can't edit or delete tag names or values with this prefix. Tags with this prefix do not count against your tags per resource limit.
Character restrictions	Tags may only contain Unicode letters, digits, whitespace, or these symbols: <code>_ . : / = + - @</code>

## Managing Tags with AWS Config API Actions

Tag based access controls are available for three resources `ConfigurationAggregator`, `AggregationAuthorization`, and `ConfigRule`. Use the following to add, update, list, and delete the tags for your resources.

- [ListTagsForResource](#)
- [TagResource](#)
- [UntagResource](#)

# Conformance Packs

A conformance pack is a collection of AWS Config rules and remediation actions that can be easily deployed as a single entity in an account and a Region or across an organization in AWS Organizations.

Conformance packs are created by authoring a YAML template that contains the list of AWS Config managed or custom rules and remediation actions. You can deploy the template by using the AWS Config console or the AWS CLI. To quickly get started and to evaluate your AWS environment, use one of the sample conformance pack templates.

## Note

Conformance packs are only available in the redesigned AWS Config console.

## Topics

- [Prerequisites \(p. 219\)](#)
- [Region Support \(p. 220\)](#)
- [AWS Config Process Checks Within a Conformance Pack \(p. 222\)](#)
- [Conformance Pack Sample Templates \(p. 225\)](#)
- [Viewing Compliance Data in the Conformance Packs Dashboard \(p. 3252\)](#)
- [Deploying a Conformance Pack Using the AWS Config Console \(p. 3252\)](#)
- [Deploying a Conformance Pack Using the AWS Command Line Interface \(p. 3254\)](#)
- [Managing Conformance Packs \(API\) \(p. 3257\)](#)
- [Managing Conformance Packs Across all Accounts in Your Organization \(p. 3257\)](#)
- [Viewing Compliance History Timeline for Conformance Packs \(p. 3258\)](#)
- [Troubleshooting \(p. 3260\)](#)

## Prerequisites

Before you deploy your conformance pack, turn on AWS Config recording.

## Start AWS Config Recording

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. Choose **Settings** in the navigation pane.
3. To start recording, under **Recording is off**, choose **Turn on**. When prompted, choose **Continue**.

## Prerequisites for Using a Conformance Pack With Remediation

Before deploying conformance packs using sample templates with remediation, you must create appropriate resources such as automation assume role and other AWS resources based on your remediation target.

If you have an existing automation role that you are using for remediation using SSM documents, you can directly provide the ARN of that role. If you have any resources you can provide those in the template.

AWS Config does not support AWS CloudFormation intrinsic functions for the automation execution role. You must provide the exact ARN of the role as a string.

For more information about how to pass the exact ARN, see [Conformance Pack Sample Templates \(p. 225\)](#). While using example templates, update your Account ID and master Account ID for organization.

## Prerequisites for Using a Conformance Pack With One or More AWS Config Rules

Before deploying a conformance pack with one or more custom AWS Config rules, create appropriate resources such as AWS Lambda function and the corresponding execution role.

If you have an existing custom AWS Config rule, you can directly provide the ARN of AWS Lambda function to create another instance of that custom rule as part of the pack.

If you do not have an existing custom AWS Config rule, you can create a AWS Lambda function and use the ARN of the Lambda function. For more information, see [AWS Config Custom Rules \(p. 193\)](#).

If your AWS Lambda function is present in a different AWS account, you can create AWS Config rules with appropriate cross-account AWS Lambda function authorization. For more information, see [How to Centrally Manage AWS Config Rules across Multiple AWS Accounts](#) blog post.

## Prerequisites for Organization Conformance Packs

Specify an automation execution role ARN for that remediation in the template if the input template has an autoremediation configuration. Ensure a role with the specified name exists in all the accounts (master and member) of an organization. You must create this role in all accounts before calling `PutOrganizationConformancePack`. You can create this role manually or using the AWS CloudFormation stack-sets to create this role in every account.

If your template uses AWS CloudFormation intrinsic function `Fn::ImportValue` to import a particular variable, then that variable must be defined as an `Export Value` in all the member accounts of that organization.

For custom AWS Config rule, see [How to Centrally Manage AWS Config Rules across Multiple AWS Accounts](#) blog to setup proper permissions.

## Region Support

Conformance packs are supported in the following Regions.

Region name	Region	Endpoint	Protocol
Asia Pacific (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asia Pacific (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia Pacific (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS

Region name	Region	Endpoint	Protocol
Asia Pacific (Singapore)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pacific (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canada (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Europe (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europe (Ireland)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europe (London)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europe (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europe (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Middle East (Bahrain)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
South America (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
US West (N. California)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS

Deploying conformance packs across member accounts in an AWS Organization is supported in the following Regions.

Region name	Region	Endpoint	Protocol
Asia Pacific (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS

Region name	Region	Endpoint	Protocol
Asia Pacific (Singapore)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pacific (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Asia Pacific (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Canada (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Europe (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europe (Ireland)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europe (London)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europe (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europe (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
South America (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
US West (N. California)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS

## AWS Config Process Checks Within a Conformance Pack

Process checks is a type of AWS Config rule that allows you to track your external and internal tasks that require verification as part of the conformance packs. These checks can be added to an existing conformance pack or a new conformance pack. You can track all compliance that includes AWS configurations and manual checks in a single location.

With process checks, you can list the compliance of requirements and actions at a single location. These process checks help increase the coverage of compliance regimes-based conformance packs. You can further expand the conformance pack by adding new process checks that track processes and actions needing manual verification and tracking. This enables conformance pack to become the template that provides details about AWS configurations and manual processes for a compliance regime.

You can track and manage the compliance of processes not associated with resource configuration changes within a conformance packs as process checks. For example, you can add a process check to track the PCI-DSS compliance requirement to store media backup at an offsite location. You will manually evaluate the compliance of this according to PCI-DSS guidelines, or according to your organization's guidance.

**Region availability:** Process checks with the conformance packs are available in all AWS Regions where AWS Config conformance packs are available. For more information, see [Region Support \(p. 220\)](#).

### Topics

- [Sample Conformance Pack Template for Creating Process Checks \(p. 223\)](#)
- [Include Process Checks Within a Conformance Pack \(p. 223\)](#)
- [Change Compliance Status of a Process Check \(p. 224\)](#)
- [View and Edit the Process Check \(Console\) \(p. 225\)](#)

## Sample Conformance Pack Template for Creating Process Checks

```
#####  
#  
# Conformance Pack template for process check  
#  
#####  
Resources:  
  AWSConfigProcessCheck:  
    Properties:  
      ConfigRuleName: RuleName  
      Description: Description of Rule  
      Source:  
        Owner: AWS  
        SourceIdentifier: AWS_CONFIG_PROCESS_CHECK  
      Type: AWS::Config::ConfigRule
```

See two sample templates, the [Operational Best Practices for CIS AWS Foundations Benchmark v1.3 Level 1 \(p. 687\)](#) template and the [Operational Best Practices for CIS AWS Foundations Benchmark v1.3 Level 2 \(p. 701\)](#) template.

## Include Process Checks Within a Conformance Pack

1. Add a process check in the conformance pack template. Refer to the previous sample template.

```
Resources:  
  ConfigEnabledAllRegions:  
    Properties:  
      ConfigRuleName: Config-Enabled-All-Regions  
      Description: Ensure AWS Config is enabled in all Regions.  
      Source:  
        Owner: AWS  
        SourceIdentifier: AWS_CONFIG_PROCESS_CHECK
```

```
Type: AWS::Config::ConfigRule
```

2. Enter the name for the process check.
3. Enter the description for the process check.
4. Deploy the conformance pack from the AWS Management Console. For more information, see [Deploying a Conformance Pack Using the AWS Config Console \(p. 3252\)](#).

**Note**

You can also deploy the conformance packs using the Command Line Interface (AWS CLI). For more information, see [Deploying a Conformance Pack Using the AWS Command Line Interface \(p. 3254\)](#).

## Change Compliance Status of a Process Check

### Change Compliance Status of a Process Check (Console)

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. Navigate to the AWS Config Rules page.
3. Choose the name of the process check that you specified in the template along with the identifier in the conformance pack.

**Note**

All the process checks from the same conformance pack have the same suffix.

4. On the Rule details page, you cannot edit the rule but you can edit the compliance of the rule. In the Manual compliance section, choose **Edit compliance**.
5. Choose the appropriate compliance from the dropdown list.
6. (Optional) Enter a description for the compliance status.
7. Choose **Save**.

After changing the compliance status, return to your conformance pack to view the process check and its description.

### Change Compliance Status of a Process Check (CLI)

You can update the compliance of process checks within a conformance pack using the AWS Command Line Interface (AWS CLI).

To install the AWS CLI on your local machine, see [Installing the AWS CLI](#) in the *AWS CLI User Guide*.

If necessary, type `aws configure` to configure the AWS CLI to use an AWS Region where AWS Config conformance packs are available.

1. Open a command prompt or a terminal window.
2. Type the following command to update the compliance of a process check where `ComplianceResourceId` is your `Account ID`, and include the name of your rule.

```
aws configservice put-external-evaluation --config-rule-  
name process-check-rule-name --external-evaluation  
ComplianceResourceType=AWS:::Account,ComplianceResourceId=Account  
ID,ComplianceType=NON_COMPLIANT,OrderingTimestamp=2020-12-17T00:10:00.000Z
```

3. Press Enter to run the command.

## Change Compliance Status of a Process Check (API)

After the deployment is complete, to update the evaluations and compliance of the process checks, use the `PutExternalEvaluation` API. For more information, see [PutExternalEvaluation](#).

## View and Edit the Process Check (Console)

You can view process checks only after a compliance state has been added to process checks. Choose the specific conformance pack to view all the process checks within that conformance pack. Here you can see a list of process checks that are in compliant and non-compliant status.

Because this is a service linked rule, you cannot edit the process check through the Rule details page.

### Note

However, you can update the compliance of the process check by choosing **Edit Compliance** and selecting the appropriate value from Compliant, Non-Compliant or Not-Applicable.

You can edit or delete a process check from the conformance pack where you added the process checks.

## Conformance Pack Sample Templates

Here are the conformance pack YAML templates that you see in AWS Config console. Within each conformance pack template, you can use one or more AWS Config rules and remediation actions. The AWS Config rules listed within the conformance pack can be AWS Config managed rules and/or AWS Config custom rules. You can download all the conformance pack templates from [GitHub](#).

### Important

Conformance packs provide a general-purpose compliance framework to help you create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. AWS conformance pack sample templates intend to help you create your own conformance packs with different or additional rules, input parameters and remediation actions that suit your environment. The sample templates, including those related to compliance standards and industry benchmarks, are not designed to ensure your compliance with a specific governance standard. They can neither replace your internal efforts nor guarantee that you will pass a compliance assessment.

### Topics

- [AWS Control Tower Detective Guardrails Conformance Pack \(p. 227\)](#)
- [Operational Best Practices for ABS CCIG 2.0 Material Workloads \(p. 227\)](#)
- [Operational Best Practices for ABS CCIG 2.0 Standard Workloads \(p. 313\)](#)
- [Operational Best Practices for ACSC Essential 8 \(p. 372\)](#)
- [Operational Best Practices for ACSC ISM \(p. 398\)](#)
- [Operational Best Practices for AI and ML \(p. 419\)](#)
- [Operational Best Practices for Amazon DynamoDB \(p. 419\)](#)
- [Operational Best Practices for Amazon S3 \(p. 419\)](#)
- [Operational Best Practices for APRA CPG 234 \(p. 420\)](#)
- [Operational Best Practices for Asset Management \(p. 513\)](#)
- [Operational Best Practices for AWS Identity And Access Management \(p. 513\)](#)
- [Operational Best Practices for AWS Well-Architected Framework Reliability Pillar \(p. 514\)](#)
- [Operational Best Practices for AWS Well-Architected Framework Security Pillar \(p. 520\)](#)
- [Operational Best Practices for BCP and DR \(p. 566\)](#)
- [Operational Best Practices for BNM RMiT \(p. 567\)](#)

- [Operational Best Practices for CIS AWS Foundations Benchmark v1.3 Level 1](#) (p. 687)
- [Operational Best Practices for CIS AWS Foundations Benchmark v1.3 Level 2](#) (p. 701)
- [Operational Best Practices for CIS Top 20](#) (p. 719)
- [Operational Best Practices for CMMC Level 1](#) (p. 758)
- [Operational Best Practices for CMMC Level 2](#) (p. 804)
- [Operational Best Practices for CMMC Level 3](#) (p. 914)
- [Operational Best Practices for CMMC Level 4](#) (p. 1049)
- [Operational Best Practices for CMMC Level 5](#) (p. 1195)
- [Operational Best Practices for Compute Services](#) (p. 1360)
- [Operational Best Practices for Data Resiliency](#) (p. 1360)
- [Operational Best Practices for Databases Services](#) (p. 1361)
- [Operational Best Practices for Data Lakes and Analytics Services](#) (p. 1361)
- [Operational Best Practices for EC2](#) (p. 1361)
- [Operational Best Practices for Encryption and Key Management](#) (p. 1361)
- [Operational Best Practices for Esquema Nacional de Seguridad \(ENS\) Low](#) (p. 1362)
- [Operational Best Practices for Esquema Nacional de Seguridad \(ENS\) Medium](#) (p. 1436)
- [Operational Best Practices for FDA Title 21 CFR Part 11](#) (p. 1528)
- [Operational Best Practices for FedRAMP\(Low\)](#) (p. 1674)
- [Operational Best Practices for FedRAMP\(Moderate\)](#) (p. 1705)
- [Operational Best Practices for FFIEC](#) (p. 1865)
- [Operational Best Practices for HIPAA Security](#) (p. 1954)
- [Operational Best Practices for K-ISMS](#) (p. 2054)
- [Operational Best Practices for Load Balancing](#) (p. 2100)
- [Operational Best Practices for Logging](#) (p. 2100)
- [Operational Best Practices for Management and Governance Services](#) (p. 2100)
- [Operational Best Practices for MAS Notice 655](#) (p. 2101)
- [Operational Best Practices for MAS TRMG June 2013](#) (p. 2116)
- [Operational Best Practices for Monitoring](#) (p. 2260)
- [Operational Best Practices for NBC TRMG](#) (p. 2260)
- [Operational Best Practices for NERC CIP](#) (p. 2522)
- [Operational Best Practices for NCSC Cloud Security Principles](#) (p. 2586)
- [Operational Best Practices for NCSC Cyber Assesment Framework](#) (p. 2608)
- [Operational Best Practices for Networking and Content Delivery Services](#) (p. 2658)
- [Operational Best Practices for NIST 800-53 rev 4](#) (p. 2658)
- [Operational Best Practices for NIST 800 171](#) (p. 2821)
- [Operational Best Practices for NIST CSF](#) (p. 2954)
- [Operational Best Practices for NYDFS 23](#) (p. 3054)
- [Operational Best Practices for PCI DSS 3.2.1](#) (p. 3122)
- [Operational Best Practices for Publicly Accessible Resources](#) (p. 3176)
- [Operational Best Practices for RBI Cyber Security Framework for UCBs](#) (p. 3177)
- [Operational Best Practices for RBI MD-ITF](#) (p. 3194)
- [Operational Best Practices for Security, Identity, and Compliance Services](#) (p. 3251)
- [Operational Best Practices for Serverless](#) (p. 3251)
- [Operational Best Practices for Storage Services](#) (p. 3251)
- [Example Templates with Remediation Action](#) (p. 3251)
- [Custom Conformance Pack](#) (p. 3252)

## AWS Control Tower Detective Guardrails Conformance Pack

The template is available on GitHub: [AWS Control Tower Detective Guardrails Conformance Pack](#).

### Operational Best Practices for ABS CCIG 2.0 Material Workloads

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the ABS Cloud Computing Implementation Guide 2.0 - Material Workloads and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more ABS Cloud Computing Implementation Guide controls. An ABS Cloud Computing Implementation Guide control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

**AWS Region:** All supported AWS Regions except Asia Pacific (Hong Kong), Europe (Stockholm), and Middle East (Bahrain)

Control ID	AWS Config Rule	Guidance
section4a-govern-the-cloud-2-standard-workloads	<a href="#">account-part-of-organizations (p. 108)</a>	Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data.
section4a-govern-the-cloud-2-standard-workloads	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
section4a-govern-the-cloud-2-standard-workloads	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
section4a-govern-the-cloud-2-standard-workloads	<a href="#">cloudtrail-security-trail-enabled (p. 118)</a>	This rule helps ensure the use of AWS recommended security best

Control ID	AWS Config Rule	Guidance
		practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions.
section4a-govern-the-cloud-2-standard-workloads	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment.
section4a-govern-the-cloud-2-standard-workloads	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
section4a-govern-the-cloud-2-standard-workloads	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	AWS Config Rule	Guidance
section4a-govern-the-cloud-2-standard-workloads	<a href="#">lambda-dlq-check (p. 161)</a>	Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed.
section4a-govern-the-cloud-2-standard-workloads	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
section4a-govern-the-cloud-2-material-workloads	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
section4a-govern-the-cloud-2-material-workloads	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	AWS Config Rule	Guidance
section4a-govern-the-cloud-3-material-workloads	<a href="#">dynamodb-throughput-limit-check (p. 130)</a>	Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set <code>accountRCUThresholdPercentage</code> (Config Default: 80) and <code>accountWCUThresholdPercentage</code> (Config Default: 80) parameters. The actual values should reflect your organization's policies.
section4a-govern-the-cloud-3-material-workloads	<a href="#">lambda-concurrency-check (p. 161)</a>	This rule ensures that a Lambda function's concurrency high and low limits are established. This can assist in baselining the number of requests that your function is serving at any given time.
section4a-govern-the-cloud-3-standard-workloads	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
section4a-govern-the-cloud-3-standard-workloads	<a href="#">ec2-security-group-attached-to-eni (p. 137)</a>	This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment.

Control ID	AWS Config Rule	Guidance
section4a-govern-the-cloud-3-standard-workloads	<a href="#">ec2-volume-inuse-check (p. 137)</a>	This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality.
section4a-govern-the-cloud-3-standard-workloads	<a href="#">eip-attached (p. 139)</a>	This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment.
section4a-govern-the-cloud-4-standard-workloads	<a href="#">account-part-of-organizations (p. 108)</a>	Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data.
section4b-design-and-secure-the-cloud-1-standard-workloads	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-1-standard-workloads	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
section4b-design-and-secure-the-cloud-1-standard-workloads	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
section4b-design-and-secure-the-cloud-2-standard-workloads	<a href="#">cloudtrail-security-trail-enabled (p. 118)</a>	This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions.
section4b-design-and-secure-the-cloud-2-standard-workloads	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-2-standard-workloads	<a href="#">ec2-managedinstance-association-compliance-status-check</a> (p. 135)	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
section4b-design-and-secure-the-cloud-2-standard-workloads	<a href="#">ec2-managedinstance-patch-compliance-status-check</a> (p. 136)	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
section4b-design-and-secure-the-cloud-2-standard-workloads	<a href="#">redshift-cluster-maintenancesettings-check</a> (p. 171)	This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the <code>allowVersionUpgrade</code> . The default is true. It also lets you optionally set the <code>preferredMaintenanceWindow</code> (the default is <code>sat:16:00-sat:16:30</code> ), and the <code>automatedSnapshotRetentionPeriod</code> (the default is 1). The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-3-standard-workloads	<a href="#">autoscaling-group-elb-healthcheck-required</a> (p. 113)	The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.
section4b-design-and-secure-the-cloud-3-standard-workloads	<a href="#">dynamodb-autoscaling-enabled</a> (p. 128)	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.
section4b-design-and-secure-the-cloud-3-standard-workloads	<a href="#">ec2-instance-detailed-monitoring-enabled</a> (p. 132)	Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance.
section4b-design-and-secure-the-cloud-3-standard-workloads	<a href="#">elb-cross-zone-load-balancing-enabled</a> (p. 143)	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-3-standard-workloads	<a href="#">rds-enhanced-monitoring-enabled (p. 165)</a>	Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics.
section4b-design-and-secure-the-cloud-3-standard-workloads	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
section4b-design-and-secure-the-cloud-3-material-workloads	<a href="#">dynamodb-autoscaling-enabled (p. 128)</a>	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-3-material-workloads	<a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a>	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.
section4b-design-and-secure-the-cloud-3-material-workloads	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
section4b-design-and-secure-the-cloud-3-material-workloads	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">alb-waf-enabled (p. 109)</a>	Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">ec2-security-group-attached-to-eni (p. 137)</a>	This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.</p>

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">rds-instance-iam-authentication-enabled (p. 166)</a>	Ensure an AWS Identity and Access Management (IAM) authentication is enabled on RDS instances to control access to systems and assets. This enforces network traffic to and from the database to be encrypted using Secure Sockets Layer (SSL). Because authentication is managed externally, you are not required to store user credentials in the database.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.
section4b-design-and-secure-the-cloud-4-material-workloads	<a href="#">alb-waf-enabled (p. 109)</a>	Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-4-material-workloads	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
section4b-design-and-secure-the-cloud-4-material-workloads	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
section4b-design-and-secure-the-cloud-4-material-workloads	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
section4b-design-and-secure-the-cloud-4-material-workloads	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
section4b-design-and-secure-the-cloud-4-material-workloads	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-4-material-workloads	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
section4b-design-and-secure-the-cloud-4-material-workloads	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
section4b-design-and-secure-the-cloud-4-material-workloads	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-4-material-workloads	<a href="#">rds-instance-public-access-check</a> (p. 166)	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
section4b-design-and-secure-the-cloud-4-material-workloads	<a href="#">redshift-cluster-public-access-check</a> (p. 171)	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
section4b-design-and-secure-the-cloud-4-material-workloads	<a href="#">restricted-common-ports</a> (p. 174)	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
section4b-design-and-secure-the-cloud-4-material-workloads	<a href="#">sagemaker-notebook-no-direct-internet-access</a> (p. 183)	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
section4b-design-and-secure-the-cloud-4-material-workloads	<a href="#">vpc-default-security-group-closed</a> (p. 188)	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-4-material-workloads	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
section4b-design-and-secure-the-cloud-4-material-workloads	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.
section4b-design-and-secure-the-cloud-5-standard-workloads	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.
section4b-design-and-secure-the-cloud-5-standard-workloads	<a href="#">cmk-backing-key-rotation-enabled (p. 123)</a>	Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-5-standard-workloads	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
section4b-design-and-secure-the-cloud-5-standard-workloads	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
section4b-design-and-secure-the-cloud-5-standard-workloads	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
section4b-design-and-secure-the-cloud-5-standard-workloads	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-5-standard-workloads	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.
section4b-design-and-secure-the-cloud-5-standard-workloads	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.
section4b-design-and-secure-the-cloud-5-standard-workloads	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
section4b-design-and-secure-the-cloud-5-material-workloads	<a href="#">cmk-backing-key-rotation-enabled (p. 123)</a>	Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-5-material-workloads	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
section4b-design-and-secure-the-cloud-5-material-workloads	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
section4b-design-and-secure-the-cloud-5-material-workloads	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
section4b-design-and-secure-the-cloud-5-material-workloads	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">alb-http-to-https-redirection-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">dynamodb-table-encrypted-kms (p. 129)</a>	Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK).
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">ec2-efs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">sagemaker-endpoint-configuration-kms-key-configured</a> (p. 182)	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">sagemaker-notebook-instance-kms-key-configured</a> (p. 183)	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">sns-encrypted-kms</a> (p. 187)	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.
section4b-design-and-secure-the-cloud-6-material-workloads	<a href="#">acm-certificate-expiration-check</a> (p. 108)	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.
section4b-design-and-secure-the-cloud-6-material-workloads	<a href="#">elb-acm-certificate-required</a> (p. 143)	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-6-material-workloads	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
section4b-design-and-secure-the-cloud-6-material-workloads	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
section4b-design-and-secure-the-cloud-6-material-workloads	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
section4b-design-and-secure-the-cloud-6-material-workloads	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-6-material-workloads	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
section4b-design-and-secure-the-cloud-6-material-workloads	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
section4b-design-and-secure-the-cloud-8-standard-workloads	<a href="#">access-keys-rotated (p. 107)</a>	The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.
section4b-design-and-secure-the-cloud-8-standard-workloads	<a href="#">account-part-of-organizations (p. 108)</a>	Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-8-standard-workloads	<a href="#">cloudtrail-security-trail-enabled (p. 118)</a>	This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions.
section4b-design-and-secure-the-cloud-8-standard-workloads	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
section4b-design-and-secure-the-cloud-8-standard-workloads	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-8-standard-workloads	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
section4b-design-and-secure-the-cloud-8-standard-workloads	<a href="#">iam-password-policy (p. 154)</a>	The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-8-standard-workloads	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
section4b-design-and-secure-the-cloud-8-standard-workloads	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
section4b-design-and-secure-the-cloud-8-standard-workloads	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
section4b-design-and-secure-the-cloud-8-standard-workloads	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-8-standard-workloads	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
section4b-design-and-secure-the-cloud-8-standard-workloads	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies.
section4b-design-and-secure-the-cloud-8-standard-workloads	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-8-standard-workloads	<a href="#">rds-instance-iam-authentication-enabled (p. 166)</a>	Ensure an AWS Identity and Access Management (IAM) authentication is enabled on RDS instances to control access to systems and assets. This enforces network traffic to and from the database to be encrypted using Secure Sockets Layer (SSL). Because authentication is managed externally, you are not required to store user credentials in the database.
section4b-design-and-secure-the-cloud-8-standard-workloads	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
section4b-design-and-secure-the-cloud-8-standard-workloads	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
section4b-design-and-secure-the-cloud-8-material-workloads	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-8-material-workloads	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
section4b-design-and-secure-the-cloud-8-material-workloads	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
section4b-design-and-secure-the-cloud-8-material-workloads	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
section4b-design-and-secure-the-cloud-8-material-workloads	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-9-standard-workloads	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
section4b-design-and-secure-the-cloud-9-standard-workloads	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
section4b-design-and-secure-the-cloud-9-standard-workloads	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
section4b-design-and-secure-the-cloud-9-standard-workloads	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-9-standard-workloads	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
section4b-design-and-secure-the-cloud-9-standard-workloads	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
section4b-design-and-secure-the-cloud-9-standard-workloads	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
section4b-design-and-secure-the-cloud-9-standard-workloads	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-9-standard-workloads	<a href="#">iam-user-unused-credentials-check</a> (p. 159)	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.
section4b-design-and-secure-the-cloud-9-standard-workloads	<a href="#">mfa-enabled-for-iam-console-access</a> (p. 163)	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
section4b-design-and-secure-the-cloud-9-standard-workloads	<a href="#">rds-instance-iam-authentication-enabled</a> (p. 166)	Ensure an AWS Identity and Access Management (IAM) authentication is enabled on RDS instances to control access to systems and assets. This enforces network traffic to and from the database to be encrypted using Secure Sockets Layer (SSL). Because authentication is managed externally, you are not required to store user credentials in the database.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-9-standard-workloads	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
section4b-design-and-secure-the-cloud-9-standard-workloads	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
section4b-design-and-secure-the-cloud-9-standard-workloads	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
section4b-design-and-secure-the-cloud-9-material-workloads	<a href="#">cloudtrail-security-trail-enabled (p. 118)</a>	This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-9-material-workloads	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
section4b-design-and-secure-the-cloud-9-material-workloads	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
section4b-design-and-secure-the-cloud-9-material-workloads	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
section4b-design-and-secure-the-cloud-9-material-workloads	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-9-material-workloads	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
section4b-design-and-secure-the-cloud-9-material-workloads	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">access-keys-rotated (p. 107)</a>	The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies.
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">mfa-enabled-for-iam-console-access</a> (p. 163)	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">rds-instance-public-access-check</a> (p. 166)	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">redshift-cluster-public-access-check</a> (p. 171)	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">restricted-common-ports</a> (p. 174)	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
section4b-design-and-secure-the-cloud-10-material-workloads	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
section4b-design-and-secure-the-cloud-10-material-workloads	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-10-material-workloads	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
section4b-design-and-secure-the-cloud-10-material-workloads	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
section4b-design-and-secure-the-cloud-10-material-workloads	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
section4b-design-and-secure-the-cloud-10-material-workloads	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-10-material-workloads	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
section4b-design-and-secure-the-cloud-10-material-workloads	<a href="#">iam-password-policy (p. 154)</a>	The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-10-material-workloads	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
section4b-design-and-secure-the-cloud-10-material-workloads	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
section4b-design-and-secure-the-cloud-10-material-workloads	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
section4b-design-and-secure-the-cloud-10-material-workloads	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-10-material-workloads	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
section4b-design-and-secure-the-cloud-10-material-workloads	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
section4b-design-and-secure-the-cloud-10-material-workloads	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
section4b-design-and-secure-the-cloud-10-material-workloads	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-10-material-workloads	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
section4b-design-and-secure-the-cloud-10-material-workloads	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
section4b-design-and-secure-the-cloud-10-material-workloads	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
section4b-design-and-secure-the-cloud-10-material-workloads	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-10-material-workloads	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
section4b-design-and-secure-the-cloud-10-material-workloads	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.
section4b-design-and-secure-the-cloud-11-material-workloads	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
section4b-design-and-secure-the-cloud-11-material-workloads	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
section4b-design-and-secure-the-cloud-11-material-workloads	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-11-material-workloads	<a href="#">cloudtrail-security-trail-enabled (p. 118)</a>	This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions.
section4b-design-and-secure-the-cloud-11-material-workloads	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment.
section4b-design-and-secure-the-cloud-11-material-workloads	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
section4b-design-and-secure-the-cloud-11-material-workloads	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-11-material-workloads	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.
section4b-design-and-secure-the-cloud-11-material-workloads	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
section4b-design-and-secure-the-cloud-11-material-workloads	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-11-material-workloads	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
section4b-design-and-secure-the-cloud-11-material-workloads	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
section4b-design-and-secure-the-cloud-11-material-workloads	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-11-material-workloads	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">codebuild-project-source-repo-url-check (p. 123)</a>	Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, user name and password within AWS Codebuild project environments. Use OAuth instead of personal access tokens or a user name and password to grant authorization for accessing GitHub or Bitbucket repositories.
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">dynamodb-table-encrypted-kms (p. 129)</a>	Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK).

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">ec2-efs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a>	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">cloudtrail-security-trail-enabled (p. 118)</a>	This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">cw-loggroup-retention-period-check (p. 125)</a>	Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.
section4b-design-and-secure-the-cloud-14-material-workloads	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
section4b-design-and-secure-the-cloud-14-material-workloads	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
section4b-design-and-secure-the-cloud-14-material-workloads	<a href="#">cloudtrail-security-trail-enabled (p. 118)</a>	This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-14-material-workloads	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
section4b-design-and-secure-the-cloud-14-material-workloads	<a href="#">cw-loggroup-retention-period-check (p. 125)</a>	Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events.
section4b-design-and-secure-the-cloud-14-material-workloads	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
section4b-design-and-secure-the-cloud-14-material-workloads	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-15-standard-workloads	<a href="#">cmk-backing-key-rotation-enabled (p. 123)</a>	Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period.
section4b-design-and-secure-the-cloud-15-standard-workloads	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
section4b-design-and-secure-the-cloud-15-standard-workloads	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
section4b-design-and-secure-the-cloud-15-standard-workloads	<a href="#">ec2-ebs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
section4b-design-and-secure-the-cloud-15-standard-workloads	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
section4b-design-and-secure-the-cloud-15-standard-workloads	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
section4b-design-and-secure-the-cloud-15-standard-workloads	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-15-standard-workloads	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.
section4b-design-and-secure-the-cloud-15-standard-workloads	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.
section4b-design-and-secure-the-cloud-15-standard-workloads	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
section4b-design-and-secure-the-cloud-15-standard-workloads	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-15-standard-workloads	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.
section4b-design-and-secure-the-cloud-15-standard-workloads	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
section4b-design-and-secure-the-cloud-15-standard-workloads	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
section4b-design-and-secure-the-cloud-15-standard-workloads	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
section4b-design-and-secure-the-cloud-15-standard-workloads	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-15-standard-workloads	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.
section4c-run-the-cloud-1-standard-workloads	<a href="#">codepipeline-deployment-count-check (p. 124)</a>	Enable this rule to help monitor unauthorized AWS CodePipeline deployments by checking for the approved deployment limit each stage can perform.
section4c-run-the-cloud-1-standard-workloads	<a href="#">codepipeline-region-fanout-check (p. 124)</a>	Enable this rule to manage and monitor development systems by enforcing deployment stage rules via region fanout factor for AWS CodePipeline.
section4c-run-the-cloud-2-standard-workloads	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
section4c-run-the-cloud-2-standard-workloads	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	AWS Config Rule	Guidance
section4c-run-the-cloud-2-standard-workloads	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
section4c-run-the-cloud-2-standard-workloads	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
section4c-run-the-cloud-2-standard-workloads	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
section4c-run-the-cloud-2-standard-workloads	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.

Control ID	AWS Config Rule	Guidance
section4c-run-the-cloud-2-standard-workloads	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
section4c-run-the-cloud-2-standard-workloads	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
section4c-run-the-cloud-2-standard-workloads	<a href="#">rds-instance-iam-authentication-enabled (p. 166)</a>	Ensure an AWS Identity and Access Management (IAM) authentication is enabled on RDS instances to control access to systems and assets. This enforces network traffic to and from the database to be encrypted using Secure Sockets Layer (SSL). Because authentication is managed externally, you are not required to store user credentials in the database.
section4c-run-the-cloud-2-standard-workloads	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	AWS Config Rule	Guidance
section4c-run-the-cloud-2-material-workloads	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
section4c-run-the-cloud-2-material-workloads	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
section4c-run-the-cloud-3-standard-workloads	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
section4c-run-the-cloud-3-standard-workloads	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
section4c-run-the-cloud-3-standard-workloads	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	AWS Config Rule	Guidance
section4c-run-the-cloud-3-standard-workloads	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
section4c-run-the-cloud-3-standard-workloads	<a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a>	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.
section4c-run-the-cloud-3-standard-workloads	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
section4c-run-the-cloud-3-standard-workloads	<a href="#">cloudtrail-security-trail-enabled (p. 118)</a>	This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions.

Control ID	AWS Config Rule	Guidance
section4c-run-the-cloud-3-standard-workloads	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
section4c-run-the-cloud-3-standard-workloads	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
section4c-run-the-cloud-3-standard-workloads	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	AWS Config Rule	Guidance
section4c-run-the-cloud-3-standard-workloads	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
section4c-run-the-cloud-3-standard-workloads	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
section4c-run-the-cloud-3-standard-workloads	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
section4c-run-the-cloud-3-standard-workloads	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
section4c-run-the-cloud-3-standard-workloads	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
section4c-run-the-cloud-3-standard-workloads	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.

Control ID	AWS Config Rule	Guidance
section4c-run-the-cloud-3-standard-workloads	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.
section4c-run-the-cloud-4-material-workloads	<a href="#">alb-waf-enabled (p. 109)</a>	Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.
section4c-run-the-cloud-4-material-workloads	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
section4c-run-the-cloud-4-material-workloads	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	AWS Config Rule	Guidance
section4c-run-the-cloud-5-standard-workloads	<a href="#">autoscaling-group-elb-healthcheck-required</a> (p. 113)	The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.
section4c-run-the-cloud-5-standard-workloads	<a href="#">cloud-trail-cloud-watch-logs-enabled</a> (p. 121)	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
section4c-run-the-cloud-5-standard-workloads	<a href="#">dynamodb-autoscaling-enabled</a> (p. 128)	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.
section4c-run-the-cloud-5-standard-workloads	<a href="#">ec2-instance-detailed-monitoring-enabled</a> (p. 132)	Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance.

Control ID	AWS Config Rule	Guidance
section4c-run-the-cloud-5-standard-workloads	<a href="#">rds-enhanced-monitoring-enabled (p. 165)</a>	Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics.
section4c-run-the-cloud-6-standard-workloads	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
section4c-run-the-cloud-6-material-workloads	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

Control ID	AWS Config Rule	Guidance
section4c-run-the-cloud-6-material-workloads	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
section4c-run-the-cloud-6-material-workloads	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
section4c-run-the-cloud-6-material-workloads	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
section4c-run-the-cloud-6-material-workloads	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.

## Template

The template is available on GitHub: [Operational Best Practices for ABS CCIIG 2.0 Material Workloads](#).

## Operational Best Practices for ABS CCIG 2.0 Standard Workloads

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the ABS Cloud Computing Implementation Guide 2.0 - Standard Workloads and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more ABS Cloud Computing Implementation Guide controls. An ABS Cloud Computing Implementation Guide control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

**AWS Region:** All supported AWS Regions except Asia Pacific (Hong Kong), Europe (Stockholm), and Middle East (Bahrain)

Control ID	AWS Config Rule	Guidance
section4a-govern-the-cloud-2-standard-workloads	<a href="#">account-part-of-organizations (p. 108)</a>	Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data.
section4a-govern-the-cloud-2-standard-workloads	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
section4a-govern-the-cloud-2-standard-workloads	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
section4a-govern-the-cloud-2-standard-workloads	<a href="#">cloudtrail-security-trail-enabled (p. 118)</a>	This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions.

Control ID	AWS Config Rule	Guidance
section4a-govern-the-cloud-2-standard-workloads	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
section4a-govern-the-cloud-2-standard-workloads	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
section4a-govern-the-cloud-2-standard-workloads	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
section4a-govern-the-cloud-2-standard-workloads	<a href="#">lambda-dlq-check (p. 161)</a>	Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed.

Control ID	AWS Config Rule	Guidance
section4a-govern-the-cloud-2-standard-workloads	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
section4a-govern-the-cloud-3-standard-workloads	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
section4a-govern-the-cloud-3-standard-workloads	<a href="#">ec2-security-group-attached-to-eni (p. 137)</a>	This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment.
section4a-govern-the-cloud-3-standard-workloads	<a href="#">ec2-volume-inuse-check (p. 137)</a>	This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality.

Control ID	AWS Config Rule	Guidance
section4a-govern-the-cloud-3-standard-workloads	<a href="#">eip-attached (p. 139)</a>	This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment.
section4a-govern-the-cloud-4-standard-workloads	<a href="#">account-part-of-organizations (p. 108)</a>	Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data.
section4b-design-and-secure-the-cloud-1-standard-workloads	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
section4b-design-and-secure-the-cloud-1-standard-workloads	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-1-standard-workloads	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
section4b-design-and-secure-the-cloud-2-standard-workloads	<a href="#">cloudtrail-security-trail-enabled (p. 118)</a>	This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions.
section4b-design-and-secure-the-cloud-2-standard-workloads	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
section4b-design-and-secure-the-cloud-2-standard-workloads	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-2-standard-workloads	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
section4b-design-and-secure-the-cloud-2-standard-workloads	<a href="#">redshift-cluster-maintenancesettings-check (p. 171)</a>	This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferredMaintenanceWindow (the default is sat:16:00-sat:16:30), and the automatedSnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies.
section4b-design-and-secure-the-cloud-3-standard-workloads	<a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a>	The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-3-standard-workloads	<a href="#">dynamodb-autoscaling-enabled (p. 128)</a>	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.
section4b-design-and-secure-the-cloud-3-standard-workloads	<a href="#">ec2-instance-detailed-monitoring-enabled (p. 132)</a>	Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance.
section4b-design-and-secure-the-cloud-3-standard-workloads	<a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a>	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.
section4b-design-and-secure-the-cloud-3-standard-workloads	<a href="#">rds-enhanced-monitoring-enabled (p. 165)</a>	Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-3-standard-workloads	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">alb-waf-enabled (p. 109)</a>	Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">ec2-security-group-attached-to-eni (p. 137)</a>	This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.</p>

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">rds-instance-iam-authentication-enabled (p. 166)</a>	Ensure an AWS Identity and Access Management (IAM) authentication is enabled on RDS instances to control access to systems and assets. This enforces network traffic to and from the database to be encrypted using Secure Sockets Layer (SSL). Because authentication is managed externally, you are not required to store user credentials in the database.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">vpc-default-security-group-closed</a> (p. 188)	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">vpc-sg-open-only-to-authorized-ports</a> (p. 189)	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
section4b-design-and-secure-the-cloud-4-standard-workloads	<a href="#">vpc-vpn-2-tunnels-up</a> (p. 189)	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.
section4b-design-and-secure-the-cloud-5-standard-workloads	<a href="#">acm-certificate-expiration-check</a> (p. 108)	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-5-standard-workloads	<a href="#">cmk-backing-key-rotation-enabled (p. 123)</a>	Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period.
section4b-design-and-secure-the-cloud-5-standard-workloads	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
section4b-design-and-secure-the-cloud-5-standard-workloads	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
section4b-design-and-secure-the-cloud-5-standard-workloads	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
section4b-design-and-secure-the-cloud-5-standard-workloads	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-5-standard-workloads	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.
section4b-design-and-secure-the-cloud-5-standard-workloads	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.
section4b-design-and-secure-the-cloud-5-standard-workloads	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">alb-http-to-https-redirection-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">dynamodb-table-encrypted-kms (p. 129)</a>	Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK).
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">ec2-efs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.
section4b-design-and-secure-the-cloud-6-standard-workloads	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.
section4b-design-and-secure-the-cloud-8-standard-workloads	<a href="#">access-keys-rotated (p. 107)</a>	The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-8-standard-workloads	<a href="#">account-part-of-organizations (p. 108)</a>	Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data.
section4b-design-and-secure-the-cloud-8-standard-workloads	<a href="#">cloudtrail-security-trail-enabled (p. 118)</a>	This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions.
section4b-design-and-secure-the-cloud-8-standard-workloads	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-8-standard-workloads	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
section4b-design-and-secure-the-cloud-8-standard-workloads	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-8-standard-workloads	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>
section4b-design-and-secure-the-cloud-8-standard-workloads	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.</p>

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-8-standard-workloads	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
section4b-design-and-secure-the-cloud-8-standard-workloads	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
section4b-design-and-secure-the-cloud-8-standard-workloads	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
section4b-design-and-secure-the-cloud-8-standard-workloads	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-8-standard-workloads	<a href="#">iam-user-unused-credentials-check</a> (p. 159)	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.
section4b-design-and-secure-the-cloud-8-standard-workloads	<a href="#">mfa-enabled-for-iam-console-access</a> (p. 163)	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
section4b-design-and-secure-the-cloud-8-standard-workloads	<a href="#">rds-instance-iam-authentication-enabled</a> (p. 166)	Ensure an AWS Identity and Access Management (IAM) authentication is enabled on RDS instances to control access to systems and assets. This enforces network traffic to and from the database to be encrypted using Secure Sockets Layer (SSL). Because authentication is managed externally, you are not required to store user credentials in the database.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-8-standard-workloads	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
section4b-design-and-secure-the-cloud-8-standard-workloads	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
section4b-design-and-secure-the-cloud-9-standard-workloads	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
section4b-design-and-secure-the-cloud-9-standard-workloads	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-9-standard-workloads	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
section4b-design-and-secure-the-cloud-9-standard-workloads	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
section4b-design-and-secure-the-cloud-9-standard-workloads	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
section4b-design-and-secure-the-cloud-9-standard-workloads	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-9-standard-workloads	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
section4b-design-and-secure-the-cloud-9-standard-workloads	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
section4b-design-and-secure-the-cloud-9-standard-workloads	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies.
section4b-design-and-secure-the-cloud-9-standard-workloads	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-9-standard-workloads	<a href="#">rds-instance-iam-authentication-enabled (p. 166)</a>	Ensure an AWS Identity and Access Management (IAM) authentication is enabled on RDS instances to control access to systems and assets. This enforces network traffic to and from the database to be encrypted using Secure Sockets Layer (SSL). Because authentication is managed externally, you are not required to store user credentials in the database.
section4b-design-and-secure-the-cloud-9-standard-workloads	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
section4b-design-and-secure-the-cloud-9-standard-workloads	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
section4b-design-and-secure-the-cloud-9-standard-workloads	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">access-keys-rotated (p. 107)</a>	The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
section4b-design-and-secure-the-cloud-10-standard-workloads	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">codebuild-project-source-repo-url-check (p. 123)</a>	Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, user name and password within AWS Codebuild project environments. Use OAuth instead of personal access tokens or a user name and password to grant authorization for accessing GitHub or Bitbucket repositories.
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">dynamodb-table-encrypted-kms (p. 129)</a>	Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK).
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">ec2-efs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.
section4b-design-and-secure-the-cloud-12-standard-workloads	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a>	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">cloudtrail-security-trail-enabled (p. 118)</a>	This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">cw-loggroup-retention-period-check (p. 125)</a>	Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-14-standard-workloads	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.
section4b-design-and-secure-the-cloud-15-standard-workloads	<a href="#">cmk-backing-key-rotation-enabled (p. 123)</a>	Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period.
section4b-design-and-secure-the-cloud-15-standard-workloads	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
section4b-design-and-secure-the-cloud-15-standard-workloads	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
section4b-design-and-secure-the-cloud-15-standard-workloads	<a href="#">ec2-ebs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
section4b-design-and-secure-the-cloud-15-standard-workloads	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-15-standard-workloads	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
section4b-design-and-secure-the-cloud-15-standard-workloads	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
section4b-design-and-secure-the-cloud-15-standard-workloads	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.
section4b-design-and-secure-the-cloud-15-standard-workloads	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.
section4b-design-and-secure-the-cloud-15-standard-workloads	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-15-standard-workloads	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.
section4b-design-and-secure-the-cloud-15-standard-workloads	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.
section4b-design-and-secure-the-cloud-15-standard-workloads	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
section4b-design-and-secure-the-cloud-15-standard-workloads	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	AWS Config Rule	Guidance
section4b-design-and-secure-the-cloud-15-standard-workloads	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
section4b-design-and-secure-the-cloud-15-standard-workloads	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
section4b-design-and-secure-the-cloud-15-standard-workloads	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.
section4c-run-the-cloud-1-standard-workloads	<a href="#">codepipeline-deployment-count-check (p. 124)</a>	Enable this rule to help monitor unauthorized AWS CodePipeline deployments by checking for the approved deployment limit each stage can perform.
section4c-run-the-cloud-1-standard-workloads	<a href="#">codepipeline-region-fanout-check (p. 124)</a>	Enable this rule to manage and monitor development systems by enforcing deployment stage rules via region fanout factor for AWS CodePipeline.

Control ID	AWS Config Rule	Guidance
section4c-run-the-cloud-2-standard-workloads	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
section4c-run-the-cloud-2-standard-workloads	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
section4c-run-the-cloud-2-standard-workloads	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
section4c-run-the-cloud-2-standard-workloads	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.

Control ID	AWS Config Rule	Guidance
section4c-run-the-cloud-2-standard-workloads	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
section4c-run-the-cloud-2-standard-workloads	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
section4c-run-the-cloud-2-standard-workloads	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
section4c-run-the-cloud-2-standard-workloads	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	AWS Config Rule	Guidance
section4c-run-the-cloud-2-standard-workloads	<a href="#">rds-instance-iam-authentication-enabled (p. 166)</a>	Ensure an AWS Identity and Access Management (IAM) authentication is enabled on RDS instances to control access to systems and assets. This enforces network traffic to and from the database to be encrypted using Secure Sockets Layer (SSL). Because authentication is managed externally, you are not required to store user credentials in the database.
section4c-run-the-cloud-2-standard-workloads	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
section4c-run-the-cloud-3-standard-workloads	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
section4c-run-the-cloud-3-standard-workloads	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
section4c-run-the-cloud-3-standard-workloads	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	AWS Config Rule	Guidance
section4c-run-the-cloud-3-standard-workloads	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
section4c-run-the-cloud-3-standard-workloads	<a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a>	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.
section4c-run-the-cloud-3-standard-workloads	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
section4c-run-the-cloud-3-standard-workloads	<a href="#">cloudtrail-security-trail-enabled (p. 118)</a>	This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions.

Control ID	AWS Config Rule	Guidance
section4c-run-the-cloud-3-standard-workloads	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
section4c-run-the-cloud-3-standard-workloads	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
section4c-run-the-cloud-3-standard-workloads	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	AWS Config Rule	Guidance
section4c-run-the-cloud-3-standard-workloads	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
section4c-run-the-cloud-3-standard-workloads	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
section4c-run-the-cloud-3-standard-workloads	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
section4c-run-the-cloud-3-standard-workloads	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
section4c-run-the-cloud-3-standard-workloads	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
section4c-run-the-cloud-3-standard-workloads	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.

Control ID	AWS Config Rule	Guidance
section4c-run-the-cloud-3-standard-workloads	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.
section4c-run-the-cloud-5-standard-workloads	<a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a>	The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.
section4c-run-the-cloud-5-standard-workloads	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
section4c-run-the-cloud-5-standard-workloads	<a href="#">dynamodb-autoscaling-enabled (p. 128)</a>	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.
section4c-run-the-cloud-5-standard-workloads	<a href="#">ec2-instance-detailed-monitoring-enabled (p. 132)</a>	Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance.

Control ID	AWS Config Rule	Guidance
section4c-run-the-cloud-5-standard-workloads	<a href="#">rds-enhanced-monitoring-enabled (p. 165)</a>	Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics.
section4c-run-the-cloud-6-standard-workloads	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

## Template

The template is available on GitHub: [Operational Best Practices for ABS CCIG 2.0 Standard Workloads](#).

## Operational Best Practices for ACSC Essential 8

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Australian Cyber Security Centre (ACSC) Essential Eight Maturity Model and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more ACSC Essential Eight controls. An ACSC Essential Eight control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings. Some of the mappings to config rules are for the higher order section (eg. Mitigation Strategies to Limit the Extent of Cyber Security Incidents) as opposed to the more prescriptive sections.

This sample conformance pack template contains mappings to controls within the ACSC Essential 8, which was created by the Commonwealth of Australia and can be found at [ACSC | Essential Eight](#). Licensing of the framework under Creative Commons Attribution 4.0 International Public License and copyright information for the framework (including a disclaimer of warranties) can be found at [ACSC | Copyright](#).

**AWS Region:** All supported AWS Regions except Asia Pacific (Hong Kong), Middle East (Bahrain), and South America (São Paulo)

Control ID	AWS Config Rule	Guidance
Mitigation_strategies_to_prevent	<a href="#">malware_delivery_and_execution_public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
Mitigation_strategies_to_prevent	<a href="#">malware_delivery_and_execution_public_ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
Mitigation_strategies_to_prevent	<a href="#">malware_delivery_and_execution_only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
Mitigation_strategies_to_prevent	<a href="#">malware_delivery_and_execution_ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
Mitigation_strategies_to_prevent	<a href="#">malware_delivery_and_execution_ec2 (p. 150)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC,

Control ID	AWS Config Rule	Guidance
		<p>without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.</p>
Mitigation_strategies_to_prevent_malware_delivery_and_execution_prohibited (p. 161)	malware_delivery_and_execution_prohibited (p. 161)	<p>Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.</p>
Mitigation_strategies_to_prevent_malware_delivery_and_execution_check (p. 166)	malware_delivery_and_execution_check (p. 166)	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.</p>
Mitigation_strategies_to_prevent_malware_delivery_and_execution_check (p. 171)	malware_delivery_and_execution_check (p. 171)	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.</p>
Mitigation_strategies_to_prevent_malware_delivery_and_execution_ports (p. 174)	malware_delivery_and_execution_ports (p. 174)	<p>Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.</p>

Control ID	AWS Config Rule	Guidance
Mitigation_strategies_to_prevent_malware_delivery_and_execution	<a href="#">malware-delivery-and-execution-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
Mitigation_strategies_to_prevent_malware_delivery_and_execution	<a href="#">malware-delivery-and-execution-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
Mitigation_strategies_to_prevent_malware_delivery_and_execution	<a href="#">malware-delivery-and-execution-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
Application_control	<a href="#">alb-waf-enabled (p. 109)</a>	Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.

Control ID	AWS Config Rule	Guidance
Application_control	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
Application_control	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
Patch_applications	<a href="#">ec2-imdsv2-check (p. 132)</a>	Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata.

Control ID	AWS Config Rule	Guidance
Patch_applications	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
Patch_applications	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
Patch_applications	<a href="#">redshift-cluster-maintenancesettings-check (p. 171)</a>	This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferredMaintenanceWindow (the default is sat:16:00-sat:16:30), and the automatedSnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
Daily_backups	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.
Daily_backups	<a href="#">dynamodb-in-backup-plan (p. 128)</a>	To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
Daily_backups	<a href="#">ebs-in-backup-plan (p. 130)</a>	To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
Daily_backups	<a href="#">efs-in-backup-plan (p. 139)</a>	To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	AWS Config Rule	Guidance
Daily_backups	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
Daily_backups	<a href="#">rds-in-backup-plan (p. 167)</a>	To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
Daily_backups	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
Daily_backups	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.

Control ID	AWS Config Rule	Guidance
Mitigation_strategies_to_limit_the_extent_of_cyber_security_incidents	<a href="#">extent_of_cyber_security_incidents_check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.
Mitigation_strategies_to_limit_the_extent_of_cyber_security_incidents	<a href="#">extent_of_cyber_security_incidents_check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
Mitigation_strategies_to_limit_the_extent_of_cyber_security_incidents	<a href="#">extent_of_cyber_security_incidents_check (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
Mitigation_strategies_to_limit_the_extent_of_cyber_security_incidents	<a href="#">extent_of_cyber_security_incidents_check (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
Mitigation_strategies_to_limit_the_extent_of_cyber_security_incidents	<a href="#">extent_of_cyber_security_incidents_check (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
Mitigation_strategies_to_limit_the_extent_of_cyber_security_incidents	<a href="#">extent_of_cyber_security_incidents_check (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	AWS Config Rule	Guidance
Mitigation_strategies_to_limit_the_extent_of_cyber-security_incidents	<a href="#">CloudTrail encryption enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
Mitigation_strategies_to_limit_the_extent_of_data-breach_incidents	<a href="#">CloudTrail log file integrity enabled (p. 122)</a>	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.
Mitigation_strategies_to_limit_the_extent_of_cyber-security_incidents	<a href="#">CloudTrail S3 bucket logging enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
Mitigation_strategies_to_limit_the_extent_of_cyber-security_incidents	<a href="#">CloudTrail S3 bucket logging encryption enabled (p. 118)</a>	This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions.
Mitigation_strategies_to_limit_the_extent_of_data-breach_incidents	<a href="#">CloudWatch Log Groups encryption enabled (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
Mitigation_strategies_to_limit_the_extent_of_cyber-security_incidents	<a href="#">DynamoDB encryption kms (p. 129)</a>	Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK).

Control ID	AWS Config Rule	Guidance
Mitigation_strategies_to_limit_the_extent_of_cybersecurity_incidents	<a href="#">extents_of_cybersecurity_default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
Mitigation_strategies_to_limit_the_extent_of_cybersecurity_incidents	<a href="#">extent_of_efs_encryption (p. 136)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
Mitigation_strategies_to_limit_the_extent_of_cybersecurity_incidents	<a href="#">extents_of_cybersecurity_in_rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
Mitigation_strategies_to_limit_the_extent_of_cybersecurity_incidents	<a href="#">extents_of_cybersecurity_encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
Mitigation_strategies_to_limit_the_extent_of_cybersecurity_incidents	<a href="#">extent_of_elb_encryption_required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
Mitigation_strategies_to_limit_the_extent_of_cybersecurity_incidents	<a href="#">extent_of_elb_logging (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	AWS Config Rule	Guidance
Mitigation_strategies_to_limit_the_extent_of_cybersecurity_incidents	<a href="#">detect_https_listeners_only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
Mitigation_strategies_to_limit_the_extent_of_cybersecurity_incidents	<a href="#">encrypt_ebs_volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
Mitigation_strategies_to_limit_the_extent_of_cybersecurity_incidents	<a href="#">centralize_guardduty_events (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
Mitigation_strategies_to_limit_the_extent_of_cybersecurity_incidents	<a href="#">iam_password_policy_requirements (p. 154)</a>	The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. To help protect credentials, this rule allows you to optionally require passwords to expire every 12 months and establish a password reuse value of 100. This policy has been configured to match requirements specified in the ACSC ISM.
Mitigation_strategies_to_limit_the_extent_of_cybersecurity_incidents	<a href="#">restrict_ssh (p. 158)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	AWS Config Rule	Guidance
Mitigation_strategies_to_limit_the_extent_of_cyber_security_incidents	internet-gateways-in-vpc-only (p. 160)	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
Mitigation_strategies_to_limit_the_extent_of_cyber_security_incidents	cloud-trail-enabled (p. 163)	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
Mitigation_strategies_to_limit_the_extent_of_cyber_security_incidents	rds-log-fileset (p. 167)	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
Mitigation_strategies_to_limit_the_extent_of_cyber_security_incidents	rds-snapshots-encrypted (p. 168)	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
Mitigation_strategies_to_limit_the_extent_of_cybersecurity_incidents	<a href="#">extent of cybersecurity incidents (p. 166)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.
Mitigation_strategies_to_limit_the_extent_of_cybersecurity_incidents	<a href="#">extent of cybersecurity incidents check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.
Mitigation_strategies_to_limit_the_extent_of_cybersecurity_incidents	<a href="#">extent of cybersecurity incidents (p. 170)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
Mitigation_strategies_to_limit_the_extent_of_cybersecurity_incidents	<a href="#">Extent of cyber security incidents blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
Mitigation_strategies_to_limit_the_extent_of_cyber-security_incidents	<a href="#">Extent of object lock enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.
Mitigation_strategies_to_limit_the_extent_of_logging_security_incidents	<a href="#">Extent of logging enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
Mitigation_strategies_to_limit_the_extent_of_cyber-security_incidents	<a href="#">Extent of cyber security prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
Mitigation_strategies_to_limit_the_extent_of_cyber-security_incidents	<a href="#">Extent of cyber security encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
Mitigation_strategies_to_limit_the_extent_of_cyber-security_incidents	<a href="#">Extent of cyber security only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	AWS Config Rule	Guidance
Mitigation_strategies_to_limit_the_extent_of_cybersecurity_incidents	<a href="#">enable-encryption-at-rest-kms (p. 182)</a>	To help protect data at rest, ensure that encryption is enabled for your S3 buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. For more information about the encryption process and administration, use the AWS Key Management Service (AWS KMS) customer-managed CMKs.
Mitigation_strategies_to_limit_the_extent_of_cybersecurity_incidents	<a href="#">enable-encryption-at-rest-sagemaker-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.
Mitigation_strategies_to_limit_the_extent_of_cybersecurity_incidents	<a href="#">enable-encryption-at-rest-sagemaker-notebook-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.
Mitigation_strategies_to_limit_the_extent_of_cybersecurity_incidents	<a href="#">enable-security-hub (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	AWS Config Rule	Guidance
Mitigation_strategies_to_limit_the_extent_of_cybersecurity_incidents	<a href="#">extent of cybersecurity incidents</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.
Mitigation_strategies_to_limit_the_extent_of_cybersecurity_incidents	<a href="#">extent of cybersecurity incidents</a> closed (p. 188)	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
Mitigation_strategies_to_limit_the_extent_of_cybersecurity_incidents	<a href="#">extent of cybersecurity incidents</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
Mitigation_strategies_to_limit_the_extent_of_cybersecurity_incidents	<a href="#">extent of cybersecurity incidents</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.

Control ID	AWS Config Rule	Guidance
Restrict_administrative_privileges	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
Restrict_administrative_privileges	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
Restrict_administrative_privileges	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
Restrict_administrative_privileges	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	AWS Config Rule	Guidance
Restrict_administrative_privileges	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies.
Restrict_administrative_privileges	<a href="#">rds-instance-iam-authentication-enabled (p. 166)</a>	Ensure an AWS Identity and Access Management (IAM) authentication is enabled on RDS instances to control access to systems and assets. This enforces network traffic to and from the database to be encrypted using Secure Sockets Layer (SSL). Because authentication is managed externally, you are not required to store user credentials in the database.
Patch_operating_systems	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
Multi-factor_authentication	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.

Control ID	AWS Config Rule	Guidance
Multi-factor_authentication	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
Multi-factor_authentication	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
Multi-factor_authentication	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
Multi-factor_authentication	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
Mitigation_strategies_to_recover_data_and_system_availability	<a href="#">api-gateway-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.

Control ID	AWS Config Rule	Guidance
Mitigation_strategies_to_recover_data_and_system_availability	data_and_system_availability-enabled (p. 121)	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
Mitigation_strategies_to_recover_data_and_system_availability	data_and_system_availability	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
Mitigation_strategies_to_recover_data_and_system_availability	data_and_system_file_availability-enabled (p. 122)	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.
Mitigation_strategies_to_recover_data_and_system_availability	data_and_system_availability-enabled (p. 118)	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
Mitigation_strategies_to_recover_data_and_system_availability	data_and_system_availability-enabled (p. 118)	This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions.

Control ID	AWS Config Rule	Guidance
Mitigation_strategies_to_recover_data_and_system_availability	data_and_system_availability_encrypted (p. 121)	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
Mitigation_strategies_to_recover_data_and_system_availability	data_and_system_availability_log_check (p. 125)	Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events.
Mitigation_strategies_to_recover_data_and_system_availability	data_and_system_availability_enabled (p. 128)	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.
Mitigation_strategies_to_recover_data_and_system_availability	data_and_system_availability_backup (p. 129)	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.
Mitigation_strategies_to_recover_data_and_system_availability	data_and_system_availability_public_check (p. 131)	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
Mitigation_strategies_to_recover_data_and_system_availability	data_and_system_availability_cross_zone_load_balancing_enabled (p. 143)	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.

Control ID	AWS Config Rule	Guidance
Mitigation_strategies_to_recover_data_and_system_availability	elasticloadbalancing:delete_protection_enabled (p. 144)	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
Mitigation_strategies_to_recover_data_and_system_availability	elasticloadbalancing:logging_enabled (p. 144)	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
Mitigation_strategies_to_recover_data_and_system_availability	cloudtrail:trail_multi_region_enabled (p. 163)	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
Mitigation_strategies_to_recover_data_and_system_availability	rds:deletion_protection_enabled (p. 164)	Ensure Amazon RDS instances have deletion protection enabled. Use deletion protection to prevent your RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.

Control ID	AWS Config Rule	Guidance
Mitigation_strategies_to_recover_data_in_a_system_availability	data-backup-enabled (p. 166)	To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
Mitigation_strategies_to_recover_data_in_a_system_availability	data-backup-enabled (p. 166) deletion-protection-enabled (p. 166)	Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
Mitigation_strategies_to_recover_data_in_a_system_availability	data-logging-enabled (p. 167)	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.

Control ID	AWS Config Rule	Guidance
Mitigation_strategies_to_recover_data_and_system_availability	data_and_system_availability	<p>Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.</p>
Mitigation_strategies_to_recover_data_and_system_availability	data_and_system_availability_prohibited (p. 168)	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.</p>
Mitigation_strategies_to_recover_data_and_system_availability	data_and_system_availability_check (p. 170)	<p>To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.</p>

Control ID	AWS Config Rule	Guidance
Mitigation_strategies_to_recover_data_and_system_availability	<a href="#">Amazon S3 bucket system availability enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.
Mitigation_strategies_to_recover_data_and_system_availability	<a href="#">Amazon S3 server access logging enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
Mitigation_strategies_to_recover_data_and_system_availability	<a href="#">Amazon VPC flow logs enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
Mitigation_strategies_to_recover_data_and_system_availability	<a href="#">AWS WAF logging enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.

## Template

The template is available on GitHub: [Operational Best Practices for ACSC Essential 8](#).

## Operational Best Practices for ACSC ISM

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Australian Cyber Security Centre (ACSC) Information Security Manual (ISM) 2020-06 and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more ISM controls. An ISM control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This Conformance Pack was validated by AWS Security Assurance Services LLC (AWS SAS), which is a team of Payment Card Industry Qualified Security Assessors (QSAs), HITRUST Certified Common Security Framework Practitioners (CSFPs), and compliance professionals certified to provide guidance and assessments for various industry frameworks. AWS SAS professionals designed this Conformance Pack to enable a customer to align to a subset of ISM.

This sample conformance pack template contains mappings to controls within the ISM framework, which was created by the Commonwealth of Australia and can be found at [Australian Government Information Security Manual](#). Licensing of the framework under Creative Commons Attribution 4.0 International Public License and copyright information for the framework (including a disclaimer of warranties) can be found at [ACSC | Copyright](#).

**AWS Region:** All supported AWS Regions except Asia Pacific (Hong Kong), Middle East (Bahrain), and South America (São Paulo)

Control ID	AWS Config Rule	Guidance
298	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
380	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
459	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for

Control ID	AWS Config Rule	Guidance
		your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
459	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
459	<a href="#">ec2-efs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
459	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
459	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
459	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
459	<a href="#">s3-default-encryption-kms (p. 182)</a>	To help protect data at rest, ensure that encryption is enabled for your S3 buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. For more information about the encryption process and administration, use the AWS Key Management Service (AWS KMS) customer-managed CMKs.

Control ID	AWS Config Rule	Guidance
586	<a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a>	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.
586	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
634	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
859	<a href="#">cw-loggroup-retention-period-check (p. 125)</a>	Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events.
974	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.

Control ID	AWS Config Rule	Guidance
974	<a href="#">mfa-enabled-for-iam-console-access</a> (p. 163)	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
1139	<a href="#">elb-custom-security-policy-ssl-check</a> (p. 143)	To help protect data in transit, ensure that your Classic ElasticLoadBalancer SSL listeners are using a custom security policy. These policies can provide various high-strength cryptographic algorithms to help ensure encrypted network communications between systems. This rule requires that you set a custom security policy for your SSL listeners. The default security policy is: Protocol-TLSv1.2,ECDHE-ECDSA-AES128-GCM-SHA256. The actual value should reflect your organization's policies.
1173	<a href="#">root-account-hardware-mfa-enabled</a> (p. 175)	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	AWS Config Rule	Guidance
1173	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
1228	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
1240	<a href="#">alb-waf-enabled (p. 109)</a>	Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.
0261	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
0261	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	AWS Config Rule	Guidance
0261	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.
1271	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
1277	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
1387	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

Control ID	AWS Config Rule	Guidance
1387	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
1402	<a href="#">iam-password-policy (p. 154)</a>	The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. To help protect credentials, this rule allows you to optionally require passwords to expire every 12 months and establish a password reuse value of 100.
1404	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies.
1405	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	AWS Config Rule	Guidance
1405	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
1405	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
1405	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.
1405	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
1410	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
1425	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
1425	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.
1425	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.
1425	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
1490	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
1490	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
1511	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.
1511	<a href="#">dynamodb-in-backup-plan (p. 128)</a>	To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	AWS Config Rule	Guidance
1511	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.
1511	<a href="#">ebs-in-backup-plan (p. 130)</a>	To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
1511	<a href="#">efs-in-backup-plan (p. 139)</a>	To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
1511	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
1512	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
1512	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
1528	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
1528	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
1528	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
1528	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.

Control ID	AWS Config Rule	Guidance
1528	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
1528	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.
1528	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.
1528	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
1528	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	AWS Config Rule	Guidance
1528	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
1528	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
1536	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
1537	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
1552	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
1552	<a href="#">alb-http-to-https-redirection-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
1552	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
1552	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
P10	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
P3	<a href="#">ec2-imdsv2-check (p. 132)</a>	Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata.

Control ID	AWS Config Rule	Guidance
P5	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
P7	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
P7	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
P8	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	AWS Config Rule	Guidance
1405	<a href="#">cloudtrail-security-trail-enabled (p. 118)</a>	This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions.
1528	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
1579	<a href="#">dynamodb-autoscaling-enabled (p. 128)</a>	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.
1425	<a href="#">dynamodb-table-encrypted-kms (p. 129)</a>	Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK).
1580	<a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a>	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.

Control ID	AWS Config Rule	Guidance
P10	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
P11	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
1528	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
1528	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	AWS Config Rule	Guidance
P1	<a href="#">rds-cluster-deletion-protection-enabled (p. 164)</a>	Ensure Amazon RDS instances have deletion protection enabled. Use deletion protection to prevent your RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
P1	<a href="#">rds-instance-deletion-protection-enabled (p. 166)</a>	Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
1277	<a href="#">rds-instance-iam-authentication-enabled (p. 166)</a>	Ensure an AWS Identity and Access Management (IAM) authentication is enabled on RDS instances to control access to systems and assets. This enforces network traffic to and from the database to be encrypted using Secure Sockets Layer (SSL). Because authentication is managed externally, you are not required to store user credentials in the database.
1511	<a href="#">rds-in-backup-plan (p. 167)</a>	To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	AWS Config Rule	Guidance
1580	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
1425	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
298	<a href="#">redshift-cluster-maintenancesettings-check (p. 171)</a>	<p>This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the <code>allowVersionUpgrade</code>. The default is <code>true</code>. It also lets you optionally set the <code>preferredMaintenanceWindow</code> (the default is <code>sat:16:00-sat:16:30</code>), and the <code>automatedSnapshotRetentionPeriod</code> (the default is <code>1</code>). The actual values should reflect your organization's policies.</p>
1388	<a href="#">restricted-common-ports (p. 174)</a>	<p>Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set <code>blockedPort1</code> - <code>blockedPort5</code> parameters (Config Defaults: <code>20,21,3389,3306,4333</code>). The actual values should reflect your organization's policies.</p>
1513	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	<p>Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.</p>

Control ID	AWS Config Rule	Guidance
1511	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.
1388	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.

## Template

The template is available on GitHub: [Operational Best Practices for ACSC ISM](#).

## Operational Best Practices for AI and ML

This pack contains AWS Config rules based on AI and ML. This Conformance Pack has been designed for compatibility with the majority of AWS regions and to not require setting of any Parameters. Additional managed rules that require parameters to be set for your environment and/or for your specific region can be found at: [List of AWS Config Managed Rules](#).

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

See Parameters section for names and descriptions of required parameters.

The template is available on GitHub: [Operational Best Practices for AI and ML](#).

## Operational Best Practices for Amazon DynamoDB

The template is available on GitHub: [Operational Best Practices for Amazon DynamoDB](#).

## Operational Best Practices for Amazon S3

The template is available on GitHub: [Operational Best Practices for Amazon S3](#).

## Operational Best Practices for APRA CPG 234

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Australian Prudential Regulation Authority (APRA) CPG 234 and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more APRA CPG 234 controls. An APRA CPG 234 control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings..

This sample conformance pack template contains mappings to controls within APRA CPG 234 2019, which was created by the Commonwealth of Australia and can be found at [Prudential Practice Guide: CPG 234 Information Security](#). Licensing of the framework under Creative Commons Australia Attribution 3.0 Licence and copyright information for the framework (including a disclaimer of warranties) can be found at [APRA | Copyright](#).

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

Control ID	AWS Config Rule	Guidance
36a	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
36a	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
36a	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon

Control ID	AWS Config Rule	Guidance
		Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
36b	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
36b	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
36b	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.

Control ID	AWS Config Rule	Guidance
36b	<a href="#">cloudtrail-security-trail-enabled (p. 118)</a>	This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions.
36c	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
36c	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
36c	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	AWS Config Rule	Guidance
36c	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
36c	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
36c	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
36c	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	AWS Config Rule	Guidance
36d	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
36d	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
36d	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
36d	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
36d	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
36d	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
36d	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
36d	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	AWS Config Rule	Guidance
36d	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
36d	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
36d	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
36d	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
36d	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.
36d	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
36d	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
36d	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.

Control ID	AWS Config Rule	Guidance
36d	<a href="#">access-keys-rotated (p. 107)</a>	<p>The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.</p>
36d	<a href="#">emr-kerberos-enabled (p. 145)</a>	<p>The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.</p>
36d	<a href="#">iam-group-has-users-check (p. 153)</a>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.</p>

Control ID	AWS Config Rule	Guidance
36d	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>
36d	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.</p>

Control ID	AWS Config Rule	Guidance
36d	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
36d	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
36d	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
36d	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	AWS Config Rule	Guidance
36d	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.
36d	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
36d	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
36d	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	AWS Config Rule	Guidance
36d	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
36d	<a href="#">ec2-imdsv2-check (p. 132)</a>	Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata.
36d	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
36e	<a href="#">secretsmanager-rotation-enabled-check (p. 183)</a>	This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised.
36e	<a href="#">secretsmanager-scheduled-rotation-success-check (p. 184)</a>	This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised.

Control ID	AWS Config Rule	Guidance
36e	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
36e	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
36e	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
36e	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
36e	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
36e	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
36e	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
36e	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	AWS Config Rule	Guidance
36e	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
36e	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
36e	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
36e	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
36e	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.
36e	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
36e	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
36e	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
36f	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
36f	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
36f	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
36f	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
36f	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
36f	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
36f	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
36f	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	AWS Config Rule	Guidance
36f	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
36f	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
36f	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
36f	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
36f	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.
36f	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
36f	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
36f	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.

Control ID	AWS Config Rule	Guidance
36f	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
36f	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
36f	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
36f	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.

Control ID	AWS Config Rule	Guidance
36f	<a href="#">alb-waf-enabled (p. 109)</a>	Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.
36g	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
36g	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
36g	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.

Control ID	AWS Config Rule	Guidance
36h	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
36h	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
36h	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.

Control ID	AWS Config Rule	Guidance
36h	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
36h	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
36h	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
36i	<a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a>	The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.

Control ID	AWS Config Rule	Guidance
36i	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
36i	<a href="#">dynamodb-throughput-limit-check (p. 130)</a>	Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set <code>accountRCUThresholdPercentage</code> (Config Default: 80) and <code>accountWCUThresholdPercentage</code> (Config Default: 80) parameters. The actual values should reflect your organization's policies.
36i	<a href="#">ec2-instance-detailed-monitoring-enabled (p. 132)</a>	Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance.

Control ID	AWS Config Rule	Guidance
36i	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
36i	<a href="#">lambda-concurrency-check (p. 161)</a>	This rule ensures that a Lambda function's concurrency high and low limits are established. This can assist in baselining the number of requests that your function is serving at any given time.
36i	<a href="#">lambda-dlq-check (p. 161)</a>	Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed.
36i	<a href="#">rds-enhanced-monitoring-enabled (p. 165)</a>	Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics.

Control ID	AWS Config Rule	Guidance
36i	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
36j	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
36j	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
36j	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.

Control ID	AWS Config Rule	Guidance
36j	<a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a>	The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.
36j	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
36j	<a href="#">dynamodb-throughput-limit-check (p. 130)</a>	Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set <code>accountRCUThresholdPercentage</code> (Config Default: 80) and <code>accountWCUThresholdPercentage</code> (Config Default: 80) parameters. The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
36j	<a href="#">ec2-instance-detailed-monitoring-enabled (p. 132)</a>	Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance.
36j	<a href="#">lambda-dlq-check (p. 161)</a>	Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed.
36j	<a href="#">rds-enhanced-monitoring-enabled (p. 165)</a>	Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics.
36l	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.

Control ID	AWS Config Rule	Guidance
36l	<a href="#">dynamodb-autoscaling-enabled (p. 128)</a>	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.
36l	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.
36l	<a href="#">ebs-optimized-instance (p. 131)</a>	An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance.
36l	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
36l	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.

Control ID	AWS Config Rule	Guidance
36l	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
36l	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
36l	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.

Control ID	AWS Config Rule	Guidance
36l	<a href="#">dynamodb-in-backup-plan (p. 128)</a>	To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
36l	<a href="#">ebs-in-backup-plan (p. 130)</a>	To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
36l	<a href="#">efs-in-backup-plan (p. 139)</a>	To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
36l	<a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a>	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.

Control ID	AWS Config Rule	Guidance
36l	<a href="#">rds-instance-deletion-protection-enabled (p. 166)</a>	Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
36l	<a href="#">rds-in-backup-plan (p. 167)</a>	To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
39(a)(b)(d)	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
39(a)(b)(d)	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.

Control ID	AWS Config Rule	Guidance
39(a)(b)(d)	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
44a	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
44a	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
44a	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	AWS Config Rule	Guidance
44b	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.
44b	<a href="#">rds-instance-deletion-protection-enabled (p. 166)</a>	Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
44b	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.
44b	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
44c	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.

Control ID	AWS Config Rule	Guidance
44c	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
45	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
45	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
45	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	AWS Config Rule	Guidance
45	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
45	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
45	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies.
45	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.

Control ID	AWS Config Rule	Guidance
45	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
45	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
45	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.

Control ID	AWS Config Rule	Guidance
45	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
45	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
45	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.

Control ID	AWS Config Rule	Guidance
45	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
45	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
45	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
45	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
45	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
45	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
45	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
45	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
45	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	AWS Config Rule	Guidance
45	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
45	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
45	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
45	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
45	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
45	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
45	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
45	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	AWS Config Rule	Guidance
45	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
45	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
45	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.

Control ID	AWS Config Rule	Guidance
47c	<a href="#">emr-kerberos-enabled (p. 145)</a>	<p>The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.</p>
47c	<a href="#">iam-group-has-users-check (p. 153)</a>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.</p>
47c	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.</p>

Control ID	AWS Config Rule	Guidance
47c	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
47c	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
47c	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
47c	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
52c	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
52c	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
52c	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
52c	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
52c	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
52c	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
52c	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.
52c	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
52c	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
52c	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.
52c	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.
52c	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.
52c	<a href="#">ec2-efs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
52c	<a href="#">dynamodb-table-encrypted-kms (p. 129)</a>	Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK).
52c	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.
52c	<a href="#">s3-default-encryption-kms (p. 182)</a>	Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data.
52d	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.

Control ID	AWS Config Rule	Guidance
52d	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.
52d	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
52d	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
52d	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
52d	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
52d	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
52d	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
52d	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
52d	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
52d	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
52d	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
52d	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	AWS Config Rule	Guidance
52d	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
52d	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
52d	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
52d	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
52e	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
52e	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
53	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
53	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
53	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
53	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
53	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
53	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
53	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
53	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
53	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
53	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
53	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
53	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.

Control ID	AWS Config Rule	Guidance
53	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
53	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
53	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
53	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
53	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
54	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.
54	<a href="#">alb-http-to-https-redirection-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
54	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
54	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
54	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
54	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).

Control ID	AWS Config Rule	Guidance
54	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
54	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
54	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
54	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.
54	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
54	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
54	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
54	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
54	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.
54	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.
54	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
54	<a href="#">ec2-efs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
54	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.
54	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
54	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
54	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
55	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	AWS Config Rule	Guidance
67	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
67	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
67	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
67	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
67	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	AWS Config Rule	Guidance
67	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	<p>AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.</p>
67	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	<p>Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.</p>
67	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	<p>The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.</p>

Control ID	AWS Config Rule	Guidance
67	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
67	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.
67	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
67	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	AWS Config Rule	Guidance
67	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
67	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
67	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.

Control ID	AWS Config Rule	Guidance
67	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
68	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
68	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
73	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	AWS Config Rule	Guidance
73	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
AttachmentA_1(b)(h)	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
AttachmentA_1(b)(h)	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	AWS Config Rule	Guidance
AttachmentA_1(b)(h)	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AttachmentA_1(b)(h)	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
AttachmentA_1(b)(h)	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AttachmentA_1(b)(h)	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
AttachmentA_1(b)(h)	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
AttachmentA_1(b)(h)	<a href="#">ec2-imdsv2-check (p. 132)</a>	Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata.
AttachmentA_1(b)(h)	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
AttachmentA_1(c)	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	AWS Config Rule	Guidance
AttachmentA_1(c)	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
AttachmentA_1(e)	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
AttachmentA_1(e)	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
AttachmentA_1(e)	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.

Control ID	AWS Config Rule	Guidance
AttachmentA_1(e)	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
AttachmentA_1(e)	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
AttachmentA_1(e)	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
AttachmentA_1(e)	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
AttachmentA_1(e)	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	AWS Config Rule	Guidance
AttachmentA_1(e)	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	<p>AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.</p>
AttachmentA_1(e)	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	<p>Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.</p>
AttachmentA_1(e)	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	<p>The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.</p>

Control ID	AWS Config Rule	Guidance
AttachmentA_1(e)	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
AttachmentA_1(e)	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.
AttachmentC_4	<a href="#">access-keys-rotated (p. 107)</a>	The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
AttachmentC_4	<a href="#">emr-kerberos-enabled (p. 145)</a>	<p>The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.</p>
AttachmentC_4	<a href="#">iam-group-has-users-check (p. 153)</a>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.</p>

Control ID	AWS Config Rule	Guidance
AttachmentC_4	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>
AttachmentC_4	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.</p>

Control ID	AWS Config Rule	Guidance
AttachmentC_4	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
AttachmentC_4	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AttachmentC_4	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
AttachmentC_4	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	AWS Config Rule	Guidance
AttachmentC_4	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.
AttachmentC_4	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
AttachmentC_4	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
AttachmentC_4	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	AWS Config Rule	Guidance
AttachmentC_4	<a href="#">secretsmanager-rotation-enabled-check (p. 183)</a>	This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised.
AttachmentC_4	<a href="#">secretsmanager-scheduled-rotation-success-check (p. 184)</a>	This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised.
AttachmentC_4	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
AttachmentC_5	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.

Control ID	AWS Config Rule	Guidance
AttachmentC_5	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
AttachmentC_5	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
AttachmentC_5	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	AWS Config Rule	Guidance
AttachmentC_5	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>
AttachmentC_6	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	<p>Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.</p>

Control ID	AWS Config Rule	Guidance
AttachmentC_6	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
AttachmentC_6	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
AttachmentC_7(c)	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
AttachmentC_7(h)	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
AttachmentC_7(h)	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	AWS Config Rule	Guidance
AttachmentC_7(h)	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
AttachmentC_7(h)	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
AttachmentC_7(h)	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment.
AttachmentC_7(h)	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	AWS Config Rule	Guidance
AttachmentC_7(h)	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
AttachmentC_7(h)	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
AttachmentC_7(h)	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	AWS Config Rule	Guidance
AttachmentC_7(h)	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
AttachmentC_7(h)	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
AttachmentC_7(h)	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
AttachmentC_7(h)	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.

Control ID	AWS Config Rule	Guidance
AttachmentC_7(i)	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.
AttachmentC_7(j)	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
AttachmentC_7(j)	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
AttachmentC_7(j)	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	AWS Config Rule	Guidance
AttachmentC_7(j)	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
AttachmentC_8	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
AttachmentC_8	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
AttachmentC_8	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
AttachmentC_8	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.

Control ID	AWS Config Rule	Guidance
AttachmentC_8	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
AttachmentC_8	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
AttachmentC_8	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	AWS Config Rule	Guidance
AttachmentC_8	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
AttachmentC_8	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
AttachmentC_8	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.
AttachmentD_1	<a href="#">codebuild-project-envvar-awscred-check (p. 123)</a>	Ensure authentication credentials <code>AWS_ACCESS_KEY_ID</code> and <code>AWS_SECRET_ACCESS_KEY</code> do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access.

Control ID	AWS Config Rule	Guidance
AttachmentD_1	<a href="#">codebuild-project-source-repo-url-check (p. 123)</a>	Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, user name and password within AWS Codebuild project environments. Use OAuth instead of personal access tokens or a user name and password to grant authorization for accessing GitHub or Bitbucket repositories.
AttachmentE_1(a)(b)(d)	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.
AttachmentE_1(a)(b)(d)	<a href="#">alb-http-to-https-redirection-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
AttachmentE_1(a)(b)(d)	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
AttachmentE_1(a)(b)(d)	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
AttachmentE_1(a)(b)(d)	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
AttachmentE_1(a)(b)(d)	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).

Control ID	AWS Config Rule	Guidance
AttachmentE_1(a)(b)(d)	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
AttachmentE_1(a)(b)(d)	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
AttachmentE_1(a)(b)(d)	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
AttachmentE_1(a)(b)(d)	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.
AttachmentE_1(a)(b)(d)	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
AttachmentE_1(a)(b)(d)	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
AttachmentE_1(a)(b)(d)	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
AttachmentE_1(a)(b)(d)	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
AttachmentE_1(a)(b)(d)	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
AttachmentE_1(a)(b)(d)	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
AttachmentE_1(a)(b)(d)	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.
AttachmentE_1(a)(b)(d)	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.
AttachmentE_1(a)(b)(d)	<a href="#">ec2-ebs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
AttachmentE_1(a)(b)(d)	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.
AttachmentE_1(a)(b)(d)	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
AttachmentE_1(a)(b)(d)	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	AWS Config Rule	Guidance
AttachmentE_1(a)(b)(d)	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
AttachmentE_4	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.
AttachmentE_4	<a href="#">cmk-backing-key-rotation-enabled (p. 123)</a>	Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period.
AttachmentE_5(d)	<a href="#">cmk-backing-key-rotation-enabled (p. 123)</a>	Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period.

## Template

The template is available on GitHub: [Operational Best Practices for APRA CPG 234](#).

## Operational Best Practices for Asset Management

This pack contains AWS Config rules based on asset management within AWS. This Conformance Pack has been designed for compatibility with the majority of AWS regions and to not require setting of any Parameters. Additional managed rules that require parameters to be set for your environment and/or for your specific region can be found at: [List of AWS Config Managed Rules](#).

See Parameters section for names and descriptions of required parameters.

The template is available on GitHub: [Operational Best Practices for Asset Management](#).

## Operational Best Practices for AWS Identity And Access Management

The template is available on GitHub: [Operational Best Practices for AWS Identity And Access Management](#).

## Operational Best Practices for AWS Well-Architected Framework Reliability Pillar

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between Amazon Web Services' Well-Architected Framework Reliability Pillar and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more of the pillar's design principles. A Well-Architected Framework category can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This Conformance Pack was validated by AWS Security Assurance Services LLC (AWS SAS), which is a team of Payment Card Industry Qualified Security Assessors (QSAs), HITRUST Certified Common Security Framework Practitioners (CCSFPs), and compliance professionals certified to provide guidance and assessments for various industry frameworks. AWS SAS professionals designed this Conformance Pack to enable a customer to align to a subset of the Well-Architected Framework Reliability Pillar design principles.

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

Control ID	Control Description	AWS Config Rule	Guidance
REL-1	How do you manage service quotas and constraints? For cloud-based workload architectures, there are service quotas (which are also referred to as service limits). These quotas exist to prevent accidentally provisioning more resources than you need and to limit request rates on API operations so as to protect services from abuse. There are also resource constraints, for example, the rate that you can push bits down a fiber-optic cable, or the amount of storage on a physical disk.	<a href="#">dynamodb-throughput-limit-check (p. 130)</a>	Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set <code>accountRCUThresholdPercentage</code> (Config Default: 80) and <code>accountWCUThresholdPercentage</code> (Config Default: 80) parameters. The actual values should reflect

Control ID	Control Description	AWS Config Rule	Guidance
			your organization's policies.
REL-1	How do you manage service quotas and constraints? For cloud-based workload architectures, there are service quotas (which are also referred to as service limits). These quotas exist to prevent accidentally provisioning more resources than you need and to limit request rates on API operations so as to protect services from abuse. There are also resource constraints, for example, the rate that you can push bits down a fiber-optic cable, or the amount of storage on a physical disk.	<a href="#">lambda-concurrency-check (p. 161)</a>	This rule ensures that a Lambda function's concurrency high and low limits are established. This can assist in baselining the number of requests that your function is serving at any given time.
REL-2	How do you plan your network topology? Workloads often exist in multiple environments. These include multiple cloud environments (both publicly accessible and private) and possibly your existing data center infrastructure. Plans must include network considerations such as intra- and inter-system connectivity, public IP address management, private IP address management, and domain name resolution.	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.

Control ID	Control Description	AWS Config Rule	Guidance
REL-7	<p>How do you design your workload to adapt to changes in demand? A scalable workload provides elasticity to add or remove resources automatically so that they closely match the current demand at any given point in time.</p>	<p><a href="#">dynamodb-autoscaling-enabled (p. 128)</a></p>	<p>Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.</p>
REL-8	<p>How do you implement change? Controlled changes are necessary to deploy new functionality, and to ensure that the workloads and the operating environment are running known software and can be patched or replaced in a predictable manner. If these changes are uncontrolled, then it makes it difficult to predict the effect of these changes, or to address issues that arise because of them.</p>	<p><a href="#">redshift-cluster-maintenancesettings-check (p. 171)</a></p>	<p>This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the <code>allowVersionUpgrade</code>. The default is true. It also lets you optionally set the <code>preferredMaintenanceWindow</code> (the default is <code>sat:16:00-sat:16:30</code>), and the <code>automatedSnapshotRetentionPeriod</code> (the default is 1). The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
REL-9	How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO).	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.
REL-9	How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO).	<a href="#">dynamodb-in-backup-plan (p. 128)</a>	To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
REL-9	How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO).	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.

Control ID	Control Description	AWS Config Rule	Guidance
REL-9	How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO).	<a href="#">ebs-in-backup-plan (p. 130)</a>	To help with data backup processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
REL-9	How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO).	<a href="#">efs-in-backup-plan (p. 139)</a>	To help with data backup processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
REL-9	How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO).	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.

Control ID	Control Description	AWS Config Rule	Guidance
REL-9	How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO).	<a href="#">rds-in-backup-plan (p. 167)</a>	To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
REL-10	How do you use fault isolation to protect your workload? Fault isolated boundaries limit the effect of a failure within a workload to a limited number of components. Components outside of the boundary are unaffected by the failure. Using multiple fault isolated boundaries, you can limit the impact on your workload.	<a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a>	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.
REL-9	How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO).	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.

Control ID	Control Description	AWS Config Rule	Guidance
REL-10	How do you use fault isolation to protect your workload? Fault isolated boundaries limit the effect of a failure within a workload to a limited number of components. Components outside of the boundary are unaffected by the failure. Using multiple fault isolated boundaries, you can limit the impact on your workload.	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.

## Template

The template is available on GitHub: [Operational Best Practices for AWS Well-Architected Reliability Pillar](#).

## Operational Best Practices for AWS Well-Architected Framework Security Pillar

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between Amazon Web Services' Well-Architected Framework Security Pillar and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more of the pillar's design principles. A Well-Architected Framework category can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This Conformance Pack was validated by AWS Security Assurance Services LLC (AWS SAS), which is a team of Payment Card Industry Qualified Security Assessors (QSAs), HITRUST Certified Common Security Framework Practitioners (CCSFPs), and compliance professionals certified to provide guidance and assessments for various industry frameworks. AWS SAS professionals designed this Conformance Pack to enable a customer to align to a subset of the Well-Architected Framework Security Pillar design principles.

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

Control ID	Control Description	AWS Config Rule	Guidance
SEC-1	How do you securely operate your workload? To operate your workload securely, you must apply overarching best practices to every area of security. Take requirements and processes that you have defined in operational excellence at an organizational and workload level, and apply them to all areas. Staying up to date with AWS and industry recommendations and threat intelligence helps you evolve your threat model and control objectives. Automating security processes, testing, and validation allow you to scale your security operations.	<a href="#">account-part-of-organizations (p. 108)</a>	Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data.
SEC-1	How do you securely operate your workload? To operate your workload securely, you must apply overarching best practices to every area of security. Take requirements and processes that you have defined in operational excellence at an organizational and workload level, and apply them to all areas. Staying up to date with AWS and industry recommendations and threat intelligence helps you evolve your threat model and control	<a href="#">codebuild-project-envvar-awscred-check (p. 123)</a>	Ensure authentication credentials <code>AWS_ACCESS_KEY_ID</code> and <code>AWS_SECRET_ACCESS_KEY</code> do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access.

Control ID	Control Description	AWS Config Rule	Guidance
	objectives. Automating security processes, testing, and validation allow you to scale your security operations.		
SEC-1	How do you securely operate your workload? To operate your workload securely, you must apply overarching best practices to every area of security. Take requirements and processes that you have defined in operational excellence at an organizational and workload level, and apply them to all areas. Staying up to date with AWS and industry recommendations and threat intelligence helps you evolve your threat model and control objectives. Automating security processes, testing, and validation allow you to scale your security operations.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.

Control ID	Control Description	AWS Config Rule	Guidance
SEC-1	<p>How do you securely operate your workload? To operate your workload securely, you must apply overarching best practices to every area of security. Take requirements and processes that you have defined in operational excellence at an organizational and workload level, and apply them to all areas. Staying up to date with AWS and industry recommendations and threat intelligence helps you evolve your threat model and control objectives. Automating security processes, testing, and validation allow you to scale your security operations.</p>	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	<p>Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.</p>
SEC-1	<p>How do you securely operate your workload? To operate your workload securely, you must apply overarching best practices to every area of security. Take requirements and processes that you have defined in operational excellence at an organizational and workload level, and apply them to all areas. Staying up to date with AWS and industry recommendations and threat intelligence helps you evolve your threat model and control objectives. Automating security processes, testing, and validation allow you to scale your security operations.</p>	<a href="#">root-account-mfa-enabled (p. 175)</a>	<p>Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SEC-2	<p>How do you manage authentication for people and machines? Authentication is required to verify the identity of someone (a person) or something (a machine). This includes administrators of your AWS accounts as well as other operators of your workload, and end users. Machine access is when one component authenticates with another, for example, an application calling an API. This includes both machines internal to your organization and external parties who need access. Understanding the type (person/machine) and relationship to your organization (internal/external) will determine how authentication (username/password, plus MFA, key/secret key, API key) will occur and where identity should be stored (root user, IAM, API Gateway, Amazon Cognito, IdP-federated).</p>	<a href="#">access-keys-rotated (p. 107)</a>	<p>The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SEC-2	<p>How do you manage authentication for people and machines? Authentication is required to verify the identity of someone (a person) or something (a machine). This includes administrators of your AWS accounts as well as other operators of your workload, and end users. Machine access is when one component authenticates with another, for example, an application calling an API. This includes both machines internal to your organization and external parties who need access. Understanding the type (person/machine) and relationship to your organization (internal/external) will determine how authentication (username/password, plus MFA, key/secret key, API key) will occur and where identity should be stored (root user, IAM, API Gateway, Amazon Cognito, IdP-federated).</p>	<p><a href="#">emr-kerberos-enabled (p. 145)</a></p>	<p>The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SEC-2	<p>How do you manage authentication for people and machines? Authentication is required to verify the identity of someone (a person) or something (a machine). This includes administrators of your AWS accounts as well as other operators of your workload, and end users. Machine access is when one component authenticates with another, for example, an application calling an API. This includes both machines internal to your organization and external parties who need access. Understanding the type (person/machine) and relationship to your organization (internal/external) will determine how authentication (username/password, plus MFA, key/secret key, API key) will occur and where identity should be stored (root user, IAM, API Gateway, Amazon Cognito, IdP-federated).</p>	<p><a href="#">iam-password-policy</a> (p. 154)</p>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SEC-2	<p>How do you manage authentication for people and machines? Authentication is required to verify the identity of someone (a person) or something (a machine). This includes administrators of your AWS accounts as well as other operators of your workload, and end users. Machine access is when one component authenticates with another, for example, an application calling an API. This includes both machines internal to your organization and external parties who need access. Understanding the type (person/machine) and relationship to your organization (internal/external) will determine how authentication (username/password, plus MFA, key/secret key, API key) will occur and where identity should be stored (root user, IAM, API Gateway, Amazon Cognito, IdP-federated).</p>	<p><a href="#">iam-user-group-membership-check (p. 157)</a></p>	<p>AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SEC-2	<p>How do you manage authentication for people and machines? Authentication is required to verify the identity of someone (a person) or something (a machine). This includes administrators of your AWS accounts as well as other operators of your workload, and end users. Machine access is when one component authenticates with another, for example, an application calling an API. This includes both machines internal to your organization and external parties who need access. Understanding the type (person/machine) and relationship to your organization (internal/external) will determine how authentication (username/password, plus MFA, key/secret key, API key) will occur and where identity should be stored (root user, IAM, API Gateway, Amazon Cognito, IdP-federated).</p>	<a href="#">iam-user-mfa-enabled (p. 158)</a>	<p>Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SEC-2	<p>How do you manage authentication for people and machines? Authentication is required to verify the identity of someone (a person) or something (a machine). This includes administrators of your AWS accounts as well as other operators of your workload, and end users. Machine access is when one component authenticates with another, for example, an application calling an API. This includes both machines internal to your organization and external parties who need access. Understanding the type (person/machine) and relationship to your organization (internal/external) will determine how authentication (username/password, plus MFA, key/secret key, API key) will occur and where identity should be stored (root user, IAM, API Gateway, Amazon Cognito, IdP-federated).</p>	<a href="#">iam-root-access-key-check (p. 157)</a>	<p>Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SEC-2	<p>How do you manage authentication for people and machines? Authentication is required to verify the identity of someone (a person) or something (a machine). This includes administrators of your AWS accounts as well as other operators of your workload, and end users. Machine access is when one component authenticates with another, for example, an application calling an API. This includes both machines internal to your organization and external parties who need access. Understanding the type (person/machine) and relationship to your organization (internal/external) will determine how authentication (username/password, plus MFA, key/secret key, API key) will occur and where identity should be stored (root user, IAM, API Gateway, Amazon Cognito, IdP-federated).</p>	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	<p>Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SEC-2	<p>How do you manage authentication for people and machines? Authentication is required to verify the identity of someone (a person) or something (a machine). This includes administrators of your AWS accounts as well as other operators of your workload, and end users. Machine access is when one component authenticates with another, for example, an application calling an API. This includes both machines internal to your organization and external parties who need access. Understanding the type (person/machine) and relationship to your organization (internal/external) will determine how authentication (username/password, plus MFA, key/secret key, API key) will occur and where identity should be stored (root user, IAM, API Gateway, Amazon Cognito, IdP-federated).</p>	<a href="#">root-account-mfa-enabled (p. 175)</a>	<p>Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SEC-2	<p>How do you manage authentication for people and machines? Authentication is required to verify the identity of someone (a person) or something (a machine). This includes administrators of your AWS accounts as well as other operators of your workload, and end users. Machine access is when one component authenticates with another, for example, an application calling an API. This includes both machines internal to your organization and external parties who need access. Understanding the type (person/machine) and relationship to your organization (internal/external) will determine how authentication (username/password, plus MFA, key/secret key, API key) will occur and where identity should be stored (root user, IAM, API Gateway, Amazon Cognito, IdP-federated).</p>	<p><a href="#">iam-user-unused-credentials-check (p. 159)</a></p>	<p>AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SEC-2	<p>How do you manage authentication for people and machines? Authentication is required to verify the identity of someone (a person) or something (a machine). This includes administrators of your AWS accounts as well as other operators of your workload, and end users. Machine access is when one component authenticates with another, for example, an application calling an API. This includes both machines internal to your organization and external parties who need access. Understanding the type (person/machine) and relationship to your organization (internal/external) will determine how authentication (username/password, plus MFA, key/secret key, API key) will occur and where identity should be stored (root user, IAM, API Gateway, Amazon Cognito, IdP-federated).</p>	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	<p>Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SEC-2	<p>How do you manage authentication for people and machines? Authentication is required to verify the identity of someone (a person) or something (a machine). This includes administrators of your AWS accounts as well as other operators of your workload, and end users. Machine access is when one component authenticates with another, for example, an application calling an API. This includes both machines internal to your organization and external parties who need access. Understanding the type (person/machine) and relationship to your organization (internal/external) will determine how authentication (username/password, plus MFA, key/secret key, API key) will occur and where identity should be stored (root user, IAM, API Gateway, Amazon Cognito, IdP-federated).</p>	<p><a href="#">secretsmanager-rotation-enabled-check (p. 183)</a></p>	<p>This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SEC-2	<p>How do you manage authentication for people and machines? Authentication is required to verify the identity of someone (a person) or something (a machine). This includes administrators of your AWS accounts as well as other operators of your workload, and end users. Machine access is when one component authenticates with another, for example, an application calling an API. This includes both machines internal to your organization and external parties who need access. Understanding the type (person/machine) and relationship to your organization (internal/external) will determine how authentication (username/password, plus MFA, key/secret key, API key) will occur and where identity should be stored (root user, IAM, API Gateway, Amazon Cognito, IdP-federated).</p>	<p><a href="#">secretsmanager-scheduled-rotation-success-check (p. 184)</a></p>	<p>This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised.</p>
SEC-3	<p>How do you manage authorization for people and machines? Authorization is the rights or permissions that you grant to people or machines to access your workload. Permissions control what someone or something has access to, including your AWS accounts, administration, internal components, APIs, end users, and more.</p>	<p><a href="#">elb-deletion-protection-enabled (p. 144)</a></p>	<p>This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SEC-3	<p>How do you manage authorization for people and machines? Authorization is the rights or permissions that you grant to people or machines to access your workload. Permissions control what someone or something has access to, including your AWS accounts, administration, internal components, APIs, end users, and more.</p>	<p><a href="#">emr-kerberos-enabled (p. 145)</a></p>	<p>The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.</p>
SEC-3	<p>How do you manage authorization for people and machines? Authorization is the rights or permissions that you grant to people or machines to access your workload. Permissions control what someone or something has access to, including your AWS accounts, administration, internal components, APIs, end users, and more.</p>	<p><a href="#">iam-group-has-users-check (p. 153)</a></p>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SEC-3	How do you manage authorization for people and machines? Authorization is the rights or permissions that you grant to people or machines to access your workload. Permissions control what someone or something has access to, including your AWS accounts, administration, internal components, APIs, end users, and more.	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
SEC-3	How do you manage authorization for people and machines? Authorization is the rights or permissions that you grant to people or machines to access your workload. Permissions control what someone or something has access to, including your AWS accounts, administration, internal components, APIs, end users, and more.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
SEC-3	How do you manage authorization for people and machines? Authorization is the rights or permissions that you grant to people or machines to access your workload. Permissions control what someone or something has access to, including your AWS accounts, administration, internal components, APIs, end users, and more.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	Control Description	AWS Config Rule	Guidance
SEC-3	How do you manage authorization for people and machines? Authorization is the rights or permissions that you grant to people or machines to access your workload. Permissions control what someone or something has access to, including your AWS accounts, administration, internal components, APIs, end users, and more.	<a href="#">rds-instance-deletion-protection-enabled (p. 166)</a>	Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
SEC-4	How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
SEC-4	How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
SEC-4	How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	Control Description	AWS Config Rule	Guidance
SEC-4	How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload.	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
SEC-4	How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload.	<a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a>	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.
SEC-4	How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.

Control ID	Control Description	AWS Config Rule	Guidance
SEC-4	How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload.	<a href="#">cloudtrail-security-trail-enabled (p. 118)</a>	This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions.
SEC-4	How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
SEC-4	How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload.	<a href="#">cw-loggroup-retention-period-check (p. 125)</a>	Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events.

Control ID	Control Description	AWS Config Rule	Guidance
SEC-4	How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
SEC-4	How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
SEC-4	How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
SEC-4	How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.

Control ID	Control Description	AWS Config Rule	Guidance
SEC-4	How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
SEC-4	How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
SEC-4	How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
SEC-4	How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.

Control ID	Control Description	AWS Config Rule	Guidance
SEC-4	How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload.	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.
SEC-5	How do you protect your network resources? Any workload that has some form of network connectivity, whether it's the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats.	<a href="#">alb-waf-enabled (p. 109)</a>	Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.
SEC-5	How do you protect your network resources? Any workload that has some form of network connectivity, whether it's the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
SEC-5	How do you protect your network resources? Any workload that has some form of network connectivity, whether itâ€™s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
SEC-5	How do you protect your network resources? Any workload that has some form of network connectivity, whether itâ€™s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
SEC-5	How do you protect your network resources? Any workload that has some form of network connectivity, whether itâ€™s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats.	<a href="#">ec2-security-group-attached-to-eni (p. 137)</a>	This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment.

Control ID	Control Description	AWS Config Rule	Guidance
SEC-5	How do you protect your network resources? Any workload that has some form of network connectivity, whether itâ€™s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
SEC-5	How do you protect your network resources? Any workload that has some form of network connectivity, whether itâ€™s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
SEC-5	How do you protect your network resources? Any workload that has some form of network connectivity, whether itâ€™s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
SEC-5	How do you protect your network resources? Any workload that has some form of network connectivity, whether itâ€™s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
SEC-5	How do you protect your network resources? Any workload that has some form of network connectivity, whether itâ€™s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.

Control ID	Control Description	AWS Config Rule	Guidance
SEC-5	How do you protect your network resources? Any workload that has some form of network connectivity, whether itâ€™s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
SEC-5	How do you protect your network resources? Any workload that has some form of network connectivity, whether itâ€™s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
SEC-5	How do you protect your network resources? Any workload that has some form of network connectivity, whether itâ€™s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
SEC-5	How do you protect your network resources? Any workload that has some form of network connectivity, whether itâ€™s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
SEC-5	How do you protect your network resources? Any workload that has some form of network connectivity, whether itâ€™s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
SEC-5	How do you protect your network resources? Any workload that has some form of network connectivity, whether itâ€™s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
SEC-5	How do you protect your network resources? Any workload that has some form of network connectivity, whether itâ€™s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
SEC-5	How do you protect your network resources? Any workload that has some form of network connectivity, whether itâ€™s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
SEC-5	How do you protect your network resources? Any workload that has some form of network connectivity, whether itâ€™s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
SEC-5	How do you protect your network resources? Any workload that has some form of network connectivity, whether itâ€™s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
SEC-6	How do you protect your compute resources? Compute resources in your workload require multiple layers of defense to help protect from external and internal threats. Compute resources include EC2 instances, containers, AWS Lambda functions, database services, IoT devices, and more.	<a href="#">ec2-imdsv2-check (p. 132)</a>	Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata.

Control ID	Control Description	AWS Config Rule	Guidance
SEC-6	How do you protect your compute resources? Compute resources in your workload require multiple layers of defense to help protect from external and internal threats. Compute resources include EC2 instances, containers, AWS Lambda functions, database services, IoT devices, and more.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
SEC-6	How do you protect your compute resources? Compute resources in your workload require multiple layers of defense to help protect from external and internal threats. Compute resources include EC2 instances, containers, AWS Lambda functions, database services, IoT devices, and more.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
SEC-6	How do you protect your compute resources? Compute resources in your workload require multiple layers of defense to help protect from external and internal threats. Compute resources include EC2 instances, containers, AWS Lambda functions, database services, IoT devices, and more.	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.

Control ID	Control Description	AWS Config Rule	Guidance
SEC-7	How do you classify your data? Classification provides a way to categorize data, based on criticality and sensitivity in order to help you determine appropriate protection and retention controls.	<a href="#">cw-loggroup-retention-period-check (p. 125)</a>	Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events.
SEC-7	How do you classify your data? Classification provides a way to categorize data, based on criticality and sensitivity in order to help you determine appropriate protection and retention controls.	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.
SEC-8	How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
SEC-8	How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.

AWS Config Developer Guide  
Operational Best Practices for AWS Well-  
Architected Framework Security Pillar

Control ID	Control Description	AWS Config Rule	Guidance
SEC-8	How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
SEC-8	How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.	<a href="#">cmk-backing-key-rotation-enabled (p. 123)</a>	Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period.
SEC-8	How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
SEC-8	How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.	<a href="#">dynamodb-table-encrypted-kms (p. 129)</a>	Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK).
SEC-8	How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
SEC-8	How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.	<a href="#">ec2-efs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
SEC-8	How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
SEC-8	How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
SEC-8	How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.

Control ID	Control Description	AWS Config Rule	Guidance
SEC-8	How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
SEC-8	How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
SEC-8	How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.

Control ID	Control Description	AWS Config Rule	Guidance
SEC-8	How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
SEC-8	How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.

Control ID	Control Description	AWS Config Rule	Guidance
SEC-8	How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
SEC-8	How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
SEC-8	How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
SEC-8	How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.
SEC-8	How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
SEC-8	How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SEC-8	<p>How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.</p>	<p><a href="#">redshift-cluster-configuration-check (p. 170)</a></p>	<p>To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.</p>
SEC-8	<p>How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.</p>	<p><a href="#">redshift-cluster-public-access-check (p. 171)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SEC-8	How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
SEC-8	How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.
SEC-8	How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
SEC-8	How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
SEC-8	How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
SEC-8	How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.
SEC-8	How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.	<a href="#">s3-default-encryption-kms (p. 182)</a>	Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SEC-8	How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.
SEC-8	How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.
SEC-8	How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
SEC-8	How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SEC-9	How do you protect your data in transit? Protect your data in transit by implementing multiple controls to reduce the risk of unauthorized access or loss.	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.
SEC-9	How do you protect your data in transit? Protect your data in transit by implementing multiple controls to reduce the risk of unauthorized access or loss.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
SEC-9	How do you protect your data in transit? Protect your data in transit by implementing multiple controls to reduce the risk of unauthorized access or loss.	<a href="#">alb-http-to-https-redirection-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
SEC-9	How do you protect your data in transit? Protect your data in transit by implementing multiple controls to reduce the risk of unauthorized access or loss.	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SEC-9	How do you protect your data in transit? Protect your data in transit by implementing multiple controls to reduce the risk of unauthorized access or loss.	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
SEC-9	How do you protect your data in transit? Protect your data in transit by implementing multiple controls to reduce the risk of unauthorized access or loss.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
SEC-9	How do you protect your data in transit? Protect your data in transit by implementing multiple controls to reduce the risk of unauthorized access or loss.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
SEC-9	How do you protect your data in transit? Protect your data in transit by implementing multiple controls to reduce the risk of unauthorized access or loss.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.

## Template

The template is available on GitHub: [Operational Best Practices for AWS Well-Architected Security Pillar](#).

## Operational Best Practices for BCP and DR

This pack contains AWS Config rules based on BCP and DR within AWS. This Conformance Pack has been designed for compatibility with the majority of AWS regions and to not require setting of any

Parameters. Additional managed rules that require parameters to be set for your environment and/or for your specific region can be found at: [List of AWS Config Managed Rules](#).

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

See Parameters section for names and descriptions of required parameters.

The template is available on GitHub: [Operational Best Practices for BCP and DR](#).

## Operational Best Practices for BNM RMiT

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Bank Negara Malaysia (BNM) Risk Management in Technology (RMiT) and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more BNM RMiT controls. A BNM RMiT control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This Conformance Pack was validated by AWS Security Assurance Services LLC (AWS SAS), which is a team of Payment Card Industry Qualified Security Assessors (QSAs), HITRUST Certified Common Security Framework Practitioners (CCSFPs), and compliance professionals certified to provide guidance and assessments for various industry frameworks. AWS SAS professionals designed this Conformance Pack to enable you to align to a subset of Title 21 CFR Part 11 design principles.

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

Control ID	Control Description	AWS Config Rule	Guidance
10.18	A financial institution must conduct due diligence and evaluate the cryptographic controls associated with the technology used in order to protect the confidentiality, integrity, authentication, authorisation and non -repudiation of information. Where a financial institution does not generate its own encryption keys, the financial institution shall undertake appropriate measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
	a reliance on third party assessments, the financial institution shall consider whether such reliance is consistent with the financial institution's risk appetite and tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted.		

Control ID	Control Description	AWS Config Rule	Guidance
10.18	<p>A financial institution must conduct due diligence and evaluate the cryptographic controls associated with the technology used in order to protect the confidentiality, integrity, authentication, authorisation and non -repudiation of information. Where a financial institution does not generate its own encryption keys, the financial institution shall undertake appropriate measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third party assessments, the financial institution shall consider whether such reliance is consistent with the financial institution's risk appetite and tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted.</p>	<p><a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a></p>	<p>To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.18	<p>A financial institution must conduct due diligence and evaluate the cryptographic controls associated with the technology used in order to protect the confidentiality, integrity, authentication, authorisation and non -repudiation of information. Where a financial institution does not generate its own encryption keys, the financial institution shall undertake appropriate measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third party assessments, the financial institution shall consider whether such reliance is consistent with the financial institution's risk appetite and tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted.</p>	<p><a href="#">cloud-trail-encryption-enabled (p. 122)</a></p>	<p>Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.18	<p>A financial institution must conduct due diligence and evaluate the cryptographic controls associated with the technology used in order to protect the confidentiality, integrity, authentication, authorisation and non -repudiation of information. Where a financial institution does not generate its own encryption keys, the financial institution shall undertake appropriate measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third party assessments, the financial institution shall consider whether such reliance is consistent with the financial institution's risk appetite and tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted.</p>	<p><a href="#">cloudwatch-log-group-encrypted (p. 121)</a></p>	<p>To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.18	<p>A financial institution must conduct due diligence and evaluate the cryptographic controls associated with the technology used in order to protect the confidentiality, integrity, authentication, authorisation and non -repudiation of information. Where a financial institution does not generate its own encryption keys, the financial institution shall undertake appropriate measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third party assessments, the financial institution shall consider whether such reliance is consistent with the financial institution's risk appetite and tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted.</p>	<p><a href="#">efs-encrypted-check (p. 138)</a></p>	<p>Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.18	<p>A financial institution must conduct due diligence and evaluate the cryptographic controls associated with the technology used in order to protect the confidentiality, integrity, authentication, authorisation and non -repudiation of information. Where a financial institution does not generate its own encryption keys, the financial institution shall undertake appropriate measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third party assessments, the financial institution shall consider whether such reliance is consistent with the financial institution's risk appetite and tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted.</p>	<p><a href="#">elasticsearch-encrypted-at-rest (p. 141)</a></p>	<p>Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.18	<p>A financial institution must conduct due diligence and evaluate the cryptographic controls associated with the technology used in order to protect the confidentiality, integrity, authentication, authorisation and non -repudiation of information. Where a financial institution does not generate its own encryption keys, the financial institution shall undertake appropriate measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third party assessments, the financial institution shall consider whether such reliance is consistent with the financial institution's risk appetite and tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted.</p>	<p><a href="#">elb-acm-certificate-required (p. 143)</a></p>	<p>Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.18	<p>A financial institution must conduct due diligence and evaluate the cryptographic controls associated with the technology used in order to protect the confidentiality, integrity, authentication, authorisation and non -repudiation of information. Where a financial institution does not generate its own encryption keys, the financial institution shall undertake appropriate measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third party assessments, the financial institution shall consider whether such reliance is consistent with the financial institution's risk appetite and tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted.</p>	<p><a href="#">encrypted-volumes (p. 146)</a></p>	<p>Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.18	<p>A financial institution must conduct due diligence and evaluate the cryptographic controls associated with the technology used in order to protect the confidentiality, integrity, authentication, authorisation and non -repudiation of information. Where a financial institution does not generate its own encryption keys, the financial institution shall undertake appropriate measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third party assessments, the financial institution shall consider whether such reliance is consistent with the financial institution's risk appetite and tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted.</p>	<p><a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a></p>	<p>To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.18	<p>A financial institution must conduct due diligence and evaluate the cryptographic controls associated with the technology used in order to protect the confidentiality, integrity, authentication, authorisation and non -repudiation of information. Where a financial institution does not generate its own encryption keys, the financial institution shall undertake appropriate measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third party assessments, the financial institution shall consider whether such reliance is consistent with the financial institution's risk appetite and tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted.</p>	<p><a href="#">rds-storage-encrypted (p. 169)</a></p>	<p>To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.18	<p>A financial institution must conduct due diligence and evaluate the cryptographic controls associated with the technology used in order to protect the confidentiality, integrity, authentication, authorisation and non -repudiation of information. Where a financial institution does not generate its own encryption keys, the financial institution shall undertake appropriate measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third party assessments, the financial institution shall consider whether such reliance is consistent with the financial institution's risk appetite and tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted.</p>	<p><a href="#">redshift-cluster-configuration-check (p. 170)</a></p>	<p>To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.18	<p>A financial institution must conduct due diligence and evaluate the cryptographic controls associated with the technology used in order to protect the confidentiality, integrity, authentication, authorisation and non -repudiation of information. Where a financial institution does not generate its own encryption keys, the financial institution shall undertake appropriate measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third party assessments, the financial institution shall consider whether such reliance is consistent with the financial institution's risk appetite and tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted.</p>	<p><a href="#">redshift-require-tls-ssl (p. 172)</a></p>	<p>Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.18	<p>A financial institution must conduct due diligence and evaluate the cryptographic controls associated with the technology used in order to protect the confidentiality, integrity, authentication, authorisation and non -repudiation of information. Where a financial institution does not generate its own encryption keys, the financial institution shall undertake appropriate measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third party assessments, the financial institution shall consider whether such reliance is consistent with the financial institution's risk appetite and tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted.</p>	<p><a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a></p>	<p>To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.18	<p>A financial institution must conduct due diligence and evaluate the cryptographic controls associated with the technology used in order to protect the confidentiality, integrity, authentication, authorisation and non -repudiation of information. Where a financial institution does not generate its own encryption keys, the financial institution shall undertake appropriate measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third party assessments, the financial institution shall consider whether such reliance is consistent with the financial institution's risk appetite and tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted.</p>	<p><a href="#">s3-bucket-ssl-requests-only (p. 181)</a></p>	<p>To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.18	<p>A financial institution must conduct due diligence and evaluate the cryptographic controls associated with the technology used in order to protect the confidentiality, integrity, authentication, authorisation and non -repudiation of information. Where a financial institution does not generate its own encryption keys, the financial institution shall undertake appropriate measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third party assessments, the financial institution shall consider whether such reliance is consistent with the financial institution's risk appetite and tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted.</p>	<p><a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a></p>	<p>To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.18	<p>A financial institution must conduct due diligence and evaluate the cryptographic controls associated with the technology used in order to protect the confidentiality, integrity, authentication, authorisation and non -repudiation of information. Where a financial institution does not generate its own encryption keys, the financial institution shall undertake appropriate measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third party assessments, the financial institution shall consider whether such reliance is consistent with the financial institution's risk appetite and tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted.</p>	<p><a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a></p>	<p>To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.18	<p>A financial institution must conduct due diligence and evaluate the cryptographic controls associated with the technology used in order to protect the confidentiality, integrity, authentication, authorisation and non -repudiation of information. Where a financial institution does not generate its own encryption keys, the financial institution shall undertake appropriate measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third party assessments, the financial institution shall consider whether such reliance is consistent with the financial institution's risk appetite and tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted.</p>	<p><a href="#">sns-encrypted-kms (p. 187)</a></p>	<p>To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.18	<p>A financial institution must conduct due diligence and evaluate the cryptographic controls associated with the technology used in order to protect the confidentiality, integrity, authentication, authorisation and non -repudiation of information. Where a financial institution does not generate its own encryption keys, the financial institution shall undertake appropriate measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third party assessments, the financial institution shall consider whether such reliance is consistent with the financial institution's risk appetite and tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted.</p>	<p><a href="#">ec2-ebs-encryption-by-default (p. 131)</a></p>	<p>To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.18	<p>A financial institution must conduct due diligence and evaluate the cryptographic controls associated with the technology used in order to protect the confidentiality, integrity, authentication, authorisation and non -repudiation of information. Where a financial institution does not generate its own encryption keys, the financial institution shall undertake appropriate measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third party assessments, the financial institution shall consider whether such reliance is consistent with the financial institution's risk appetite and tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted.</p>	<p><a href="#">rds-snapshot-encrypted (p. 168)</a></p>	<p>Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.18	<p>A financial institution must conduct due diligence and evaluate the cryptographic controls associated with the technology used in order to protect the confidentiality, integrity, authentication, authorisation and non -repudiation of information. Where a financial institution does not generate its own encryption keys, the financial institution shall undertake appropriate measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third party assessments, the financial institution shall consider whether such reliance is consistent with the financial institution's risk appetite and tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted.</p>	<p><a href="#">cmk-backing-key-rotation-enabled (p. 123)</a></p>	<p>Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.18	<p>A financial institution must conduct due diligence and evaluate the cryptographic controls associated with the technology used in order to protect the confidentiality, integrity, authentication, authorisation and non -repudiation of information. Where a financial institution does not generate its own encryption keys, the financial institution shall undertake appropriate measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third party assessments, the financial institution shall consider whether such reliance is consistent with the financial institution's risk appetite and tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted.</p>	<p><a href="#">s3-default-encryption-kms (p. 182)</a></p>	<p>Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.18	<p>A financial institution must conduct due diligence and evaluate the cryptographic controls associated with the technology used in order to protect the confidentiality, integrity, authentication, authorisation and non -repudiation of information. Where a financial institution does not generate its own encryption keys, the financial institution shall undertake appropriate measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third party assessments, the financial institution shall consider whether such reliance is consistent with the financial institution's risk appetite and tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted.</p>	<p><a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a></p>	<p>Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.18	<p>A financial institution must conduct due diligence and evaluate the cryptographic controls associated with the technology used in order to protect the confidentiality, integrity, authentication, authorisation and non -repudiation of information. Where a financial institution does not generate its own encryption keys, the financial institution shall undertake appropriate measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third party assessments, the financial institution shall consider whether such reliance is consistent with the financial institution's risk appetite and tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted.</p>	<p><a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a></p>	<p>Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.18	<p>A financial institution must conduct due diligence and evaluate the cryptographic controls associated with the technology used in order to protect the confidentiality, integrity, authentication, authorisation and non -repudiation of information. Where a financial institution does not generate its own encryption keys, the financial institution shall undertake appropriate measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third party assessments, the financial institution shall consider whether such reliance is consistent with the financial institution's risk appetite and tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted.</p>	<p><a href="#">elb-tls-https-listeners-only (p. 145)</a></p>	<p>Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.2	<p>A financial institution shall store public cryptographic keys in a certificate issued by a certificate authority as appropriate to the level of risk. Such certificates associated with customers shall be issued by recognised certificate authorities. The financial institution must ensure that the implementation of authentication and signature protocols using such certificates are subject to strong protection to ensure that the use of private cryptographic keys corresponding to the user certificates are legally binding and irrefutable. The initial issuance and subsequent renewal of such certificates must be consistent with industry best practices and applicable legal/regulatory specifications.</p>	<p><a href="#">elb-acm-certificate-required (p. 143)</a></p>	<p>Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.2	<p>A financial institution shall store public cryptographic keys in a certificate issued by a certificate authority as appropriate to the level of risk. Such certificates associated with customers shall be issued by recognised certificate authorities. The financial institution must ensure that the implementation of authentication and signature protocols using such certificates are subject to strong protection to ensure that the use of private cryptographic keys corresponding to the user certificates are legally binding and irrefutable. The initial issuance and subsequent renewal of such certificates must be consistent with industry best practices and applicable legal/regulatory specifications.</p>	<p><a href="#">acm-certificate-expiration-check (p. 108)</a></p>	<p>Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.27	A financial institution must establish real-time monitoring mechanisms to track capacity utilisation and performance of key processes and services. These monitoring mechanisms shall be capable of providing timely and actionable alerts to administrators.	<a href="#">cloudwatch-alarm-resource-check (p. 120)</a>	Enable this rule to check whether the specified resource type has an Amazon CloudWatch alarm for the specified metric. For resource type, you can specify EBS volumes, EC2 instances, RDS clusters, or S3 buckets. Use CloudWatch alarms for communicating event detection information to appropriate personnel. This rule requires you to set resourceType (for example, AWS::EC2::Instance) and metricName (for example, CPUUtilization) parameters.
10.27	A financial institution must establish real-time monitoring mechanisms to track capacity utilisation and performance of key processes and services. These monitoring mechanisms shall be capable of providing timely and actionable alerts to administrators.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
10.27	A financial institution must establish real-time monitoring mechanisms to track capacity utilisation and performance of key processes and services. These monitoring mechanisms shall be capable of providing timely and actionable alerts to administrators.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), and <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
10.27	A financial institution must establish real-time monitoring mechanisms to track capacity utilisation and performance of key processes and services. These monitoring mechanisms shall be capable of providing timely and actionable alerts to administrators.	<a href="#">ec2-instance-detailed-monitoring-enabled (p. 132)</a>	Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance.

Control ID	Control Description	AWS Config Rule	Guidance
10.27	A financial institution must establish real-time monitoring mechanisms to track capacity utilisation and performance of key processes and services. These monitoring mechanisms shall be capable of providing timely and actionable alerts to administrators.	<a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a>	The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.
10.27	A financial institution must establish real-time monitoring mechanisms to track capacity utilisation and performance of key processes and services. These monitoring mechanisms shall be capable of providing timely and actionable alerts to administrators.	<a href="#">rds-enhanced-monitoring-enabled (p. 165)</a>	Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics.

Control ID	Control Description	AWS Config Rule	Guidance
10.27	A financial institution must establish real-time monitoring mechanisms to track capacity utilisation and performance of key processes and services. These monitoring mechanisms shall be capable of providing timely and actionable alerts to administrators.	<a href="#">lambda-concurrency-check (p. 161)</a>	This rule ensures that a Lambda function's concurrency high and low limits are established. This can assist in baselining the number of requests that your function is serving at any given time.
10.27	A financial institution must establish real-time monitoring mechanisms to track capacity utilisation and performance of key processes and services. These monitoring mechanisms shall be capable of providing timely and actionable alerts to administrators.	<a href="#">dynamodb-throughput-limit-check (p. 130)</a>	Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set <code>accountRCUThresholdPercentage</code> (Config Default: 80) and <code>accountWCUThresholdPercentage</code> (Config Default: 80) parameters. The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
10.34	A financial institution must ensure the network services for its critical systems are reliable and have no SPOF in order to protect the critical systems against potential network faults and cyber threats.	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.
10.34	A financial institution must ensure the network services for its critical systems are reliable and have no SPOF in order to protect the critical systems against potential network faults and cyber threats.	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
10.35	A financial institution must establish real-time network bandwidth monitoring processes and corresponding network service resilience metrics to flag any over utilisation of bandwidth and system disruptions due to bandwidth congestion and network faults. This includes traffic analysis to detect trends and anomalies.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.

Control ID	Control Description	AWS Config Rule	Guidance
10.35	A financial institution must establish real-time network bandwidth monitoring processes and corresponding network service resilience metrics to flag any over utilisation of bandwidth and system disruptions due to bandwidth congestion and network faults. This includes traffic analysis to detect trends and anomalies.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
10.35	A financial institution must establish real-time network bandwidth monitoring processes and corresponding network service resilience metrics to flag any over utilisation of bandwidth and system disruptions due to bandwidth congestion and network faults. This includes traffic analysis to detect trends and anomalies.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
10.36	A financial institution must ensure network services supporting critical systems are designed and implemented to ensure the confidentiality, integrity and availability of data.	<a href="#">alb-http-to-https-redirection-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
10.36	A financial institution must ensure network services supporting critical systems are designed and implemented to ensure the confidentiality, integrity and availability of data.	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
10.36	A financial institution must ensure network services supporting critical systems are designed and implemented to ensure the confidentiality, integrity and availability of data.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
10.36	A financial institution must ensure network services supporting critical systems are designed and implemented to ensure the confidentiality, integrity and availability of data.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
10.36	A financial institution must ensure network services supporting critical systems are designed and implemented to ensure the confidentiality, integrity and availability of data.	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.

Control ID	Control Description	AWS Config Rule	Guidance
10.36	A financial institution must ensure network services supporting critical systems are designed and implemented to ensure the confidentiality, integrity and availability of data.	<a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a>	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.
10.38	A financial institution must ensure sufficient and relevant network device logs are retained for investigations and forensic purposes for at least three years.	<a href="#">cw-loggroup-retention-period-check (p. 125)</a>	Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events.

Control ID	Control Description	AWS Config Rule	Guidance
10.53	A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.

Control ID	Control Description	AWS Config Rule	Guidance
10.53	A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	Control Description	AWS Config Rule	Guidance
10.53	<p>A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.</p>	<p><a href="#">iam-password-policy (p. 154)</a></p>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. To help protect credentials, this rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.53	A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
10.53	A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.

Control ID	Control Description	AWS Config Rule	Guidance
10.53	<p>A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.</p>	<p><a href="#">iam-user-group-membership-check (p. 157)</a></p>	<p>AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.</p>
10.53	<p>A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.</p>	<p><a href="#">iam-user-mfa-enabled (p. 158)</a></p>	<p>Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.53	<p>A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.</p>	<p><a href="#">iam-user-no-policies-check (p. 158)</a></p>	<p>This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.</p>
10.53	<p>A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.</p>	<p><a href="#">iam-user-unused-credentials-check (p. 159)</a></p>	<p>AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.53	A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
10.53	A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	Control Description	AWS Config Rule	Guidance
10.53	A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
10.53	A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.

Control ID	Control Description	AWS Config Rule	Guidance
10.53	<p>A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.</p>	<p><a href="#">iam-no-inline-policy-check (p. 154)</a></p>	<p>Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.</p>
10.53	<p>A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.</p>	<p><a href="#">dms-replication-not-public (p. 127)</a></p>	<p>Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.53	A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
10.53	A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
10.53	<p>A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.</p>	<p><a href="#">elasticsearch-in-vpc-only (p. 141)</a></p>	<p>Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.</p>
10.53	<p>A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.</p>	<p><a href="#">emr-master-no-public-ip (p. 146)</a></p>	<p>Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.53	<p>A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.</p>	<p><a href="#">ec2-instances-in-vpc (p. 159)</a></p>	<p>Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.</p>
10.53	<p>A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.</p>	<p><a href="#">internet-gateway-authorized-vpc-only (p. 160)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.53	A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
10.53	A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.

Control ID	Control Description	AWS Config Rule	Guidance
10.53	A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
10.53	A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
10.53	<p>A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.</p>	<p><a href="#">redshift-cluster-public-access-check (p. 171)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.</p>
10.53	<p>A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.</p>	<p><a href="#">s3-account-level-public-access-blocks (p. 175)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.53	A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
10.53	A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
10.53	A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
10.53	A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
10.53	A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
10.53	A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.

Control ID	Control Description	AWS Config Rule	Guidance
10.53	A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
10.53	A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.

Control ID	Control Description	AWS Config Rule	Guidance
10.53	<p>A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.</p>	<p><a href="#">encrypted-volumes (p. 146)</a></p>	<p>Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.</p>
10.53	<p>A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.</p>	<p><a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a></p>	<p>To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.53	<p>A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.</p>	<p><a href="#">rds-storage-encrypted (p. 169)</a></p>	<p>To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.</p>
10.53	<p>A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.</p>	<p><a href="#">redshift-cluster-configuration-check (p. 170)</a></p>	<p>To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.53	<p>A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.</p>	<p><a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a></p>	<p>To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.</p>
10.53	<p>A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.</p>	<p><a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a></p>	<p>To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.53	<p>A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.</p>	<p><a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a></p>	<p>To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.</p>
10.53	<p>A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.</p>	<p><a href="#">sns-encrypted-kms (p. 187)</a></p>	<p>To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.53	A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.	<a href="#">ec2-ebs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
10.53	A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
10.53	A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.	<a href="#">cmk-backing-key-rotation-enabled (p. 123)</a>	Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period.
10.53	A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.	<a href="#">s3-default-encryption-kms (p. 182)</a>	Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
10.53	A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
10.53	A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
10.53	A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
10.53	A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
10.53	A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
10.53	A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
10.53	<p>A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.</p>	<p><a href="#">elb-tls-https-listeners-only (p. 145)</a></p>	<p>Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.</p>
10.54	<p>A financial institution must implement an appropriate access controls policy for the identification, authentication and authorisation of users (internal and external users such as third party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems.</p>	<p><a href="#">iam-user-unused-credentials-check (p. 159)</a></p>	<p>AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.54	<p>A financial institution must implement an appropriate access controls policy for the identification, authentication and authorisation of users (internal and external users such as third party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems</p>	<p><a href="#">emr-kerberos-enabled (p. 145)</a></p>	<p>The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.</p>
10.54	<p>A financial institution must implement an appropriate access controls policy for the identification, authentication and authorisation of users (internal and external users such as third party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems</p>	<p><a href="#">iam-group-has-users-check (p. 153)</a></p>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.54	<p>A financial institution must implement an appropriate access controls policy for the identification, authentication and authorisation of users (internal and external users such as third party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems</p>	<p><a href="#">iam-password-policy (p. 154)</a></p>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. To help protect credentials, this rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.54	A financial institution must implement an appropriate access controls policy for the identification, authentication and authorisation of users (internal and external users such as third party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
10.54	A financial institution must implement an appropriate access controls policy for the identification, authentication and authorisation of users (internal and external users such as third party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.

Control ID	Control Description	AWS Config Rule	Guidance
10.54	A financial institution must implement an appropriate access controls policy for the identification, authentication and authorisation of users (internal and external users such as third party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
10.54	A financial institution must implement an appropriate access controls policy for the identification, authentication and authorisation of users (internal and external users such as third party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.

Control ID	Control Description	AWS Config Rule	Guidance
10.54	A financial institution must implement an appropriate access controls policy for the identification, authentication and authorisation of users (internal and external users such as third party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
10.54	A financial institution must implement an appropriate access controls policy for the identification, authentication and authorisation of users (internal and external users such as third party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
10.54	A financial institution must implement an appropriate access controls policy for the identification, authentication and authorisation of users (internal and external users such as third party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
10.54	A financial institution must implement an appropriate access controls policy for the identification, authentication and authorisation of users (internal and external users such as third party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	Control Description	AWS Config Rule	Guidance
10.54	A financial institution must implement an appropriate access controls policy for the identification, authentication and authorisation of users (internal and external users such as third party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
10.54	A financial institution must implement an appropriate access controls policy for the identification, authentication and authorisation of users (internal and external users such as third party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.

Control ID	Control Description	AWS Config Rule	Guidance
10.55(b)	<p>In observing paragraph 10.54, a financial institution should consider the following principles in its access control policy: (b) employ “least privilege” access rights or on a ‘need-to-have’ basis where only the minimum sufficient permissions are granted to legitimate users to perform their roles;</p>	<p><a href="#">emr-kerberos-enabled (p. 145)</a></p>	<p>The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.</p>
10.55(b)	<p>In observing paragraph 10.54, a financial institution should consider the following principles in its access control policy: (b) employ “least privilege” access rights or on a ‘need-to-have’ basis where only the minimum sufficient permissions are granted to legitimate users to perform their roles;</p>	<p><a href="#">iam-group-has-users-check (p. 153)</a></p>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.55(b)	In observing paragraph 10.54, a financial institution should consider the following principles in its access control policy: (b) employ "least privilege" access rights or on a 'need-to-have' basis where only the minimum sufficient permissions are granted to legitimate users to perform their roles;	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
10.55(b)	In observing paragraph 10.54, a financial institution should consider the following principles in its access control policy: (b) employ "least privilege" access rights or on a 'need-to-have' basis where only the minimum sufficient permissions are granted to legitimate users to perform their roles;	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
10.55(b)	In observing paragraph 10.54, a financial institution should consider the following principles in its access control policy: (b) employ "least privilege" access rights or on a 'need-to-have' basis where only the minimum sufficient permissions are granted to legitimate users to perform their roles;	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	Control Description	AWS Config Rule	Guidance
10.55(b)	In observing paragraph 10.54, a financial institution should consider the following principles in its access control policy: (b) employ “least privilege” access rights or on a ‘need-to-have’ basis where only the minimum sufficient permissions are granted to legitimate users to perform their roles;	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
10.55(b)	In observing paragraph 10.54, a financial institution should consider the following principles in its access control policy: (b) employ “least privilege” access rights or on a ‘need-to-have’ basis where only the minimum sufficient permissions are granted to legitimate users to perform their roles;	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
10.55(b)(h)(i)	In observing paragraph 10.54, a financial institution should consider the following principles in its access control policy: (b) employ “least privilege” access rights or on a ‘need-to-have’ basis where only the minimum (h) limit and control the sharing of user ID and passwords across multiple users; and (i) control the use of generic user ID naming conventions in favour of more personally identifiable IDs.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.

Control ID	Control Description	AWS Config Rule	Guidance
10.55(c)(f)	<p>In observing paragraph 10.54, a financial institution should consider the following principles in its access control policy: (c) employ time-bound access rights which restrict access to a specific period including access rights granted to service providers; (f) adopt stronger authentication for critical activities including for remote access</p>	<p><a href="#">iam-password-policy (p. 154)</a></p>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. To help protect credentials, this rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.55(f)(h)	In observing paragraph 10.54, a financial institution should consider the following principles in its access control policy: (f) adopt stronger authentication for critical activities including for remote access; (h) limit and control the sharing of user ID and passwords across multiple users	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
10.55(f)(h)	In observing paragraph 10.54, a financial institution should consider the following principles in its access control policy: (f) adopt stronger authentication for critical activities including for remote access; (h) limit and control the sharing of user ID and passwords across multiple users	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
10.55(f)(h)	In observing paragraph 10.54, a financial institution should consider the following principles in its access control policy: (f) adopt stronger authentication for critical activities including for remote access; (h) limit and control the sharing of user ID and passwords across multiple users	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	Control Description	AWS Config Rule	Guidance
10.55(f)(h)	<p>In observing paragraph 10.54, a financial institution should consider the following principles in its access control policy: (f) adopt stronger authentication for critical activities including for remote access; (h) limit and control the sharing of user ID and passwords across multiple users</p>	<p><a href="#">root-account-mfa-enabled (p. 175)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.</p>
10.56	<p>A financial institution must employ robust authentication processes to ensure the authenticity of identities in use. Authentication mechanisms shall be commensurate with the criticality of the functions and adopt at least one or more of these three basic authentication factors, namely, something the user knows (e.g. password, PIN), something the user possesses (e.g. smart card, security device) and something the user is (e.g. biometric characteristics, such as a fingerprint or retinal pattern).</p>	<p><a href="#">iam-user-mfa-enabled (p. 158)</a></p>	<p>Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.56	<p>A financial institution must employ robust authentication processes to ensure the authenticity of identities in use. Authentication mechanisms shall be commensurate with the criticality of the functions and adopt at least one or more of these three basic authentication factors, namely, something the user knows (e.g. password, PIN), something the user possesses (e.g. smart card, security device) and something the user is (e.g. biometric characteristics, such as a fingerprint or retinal pattern).</p>	<p><a href="#">root-account-hardware-mfa-enabled (p. 175)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.</p>
10.56	<p>A financial institution must employ robust authentication processes to ensure the authenticity of identities in use. Authentication mechanisms shall be commensurate with the criticality of the functions and adopt at least one or more of these three basic authentication factors, namely, something the user knows (e.g. password, PIN), something the user possesses (e.g. smart card, security device) and something the user is (e.g. biometric characteristics, such as a fingerprint or retinal pattern).</p>	<p><a href="#">root-account-mfa-enabled (p. 175)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.56	<p>A financial institution must employ robust authentication processes to ensure the authenticity of identities in use. Authentication mechanisms shall be commensurate with the criticality of the functions and adopt at least one or more of these three basic authentication factors, namely, something the user knows (e.g. password, PIN), something the user possesses (e.g. smart card, security device) and something the user is (e.g. biometric characteristics, such as a fingerprint or retinal pattern).</p>	<p><a href="#">mfa-enabled-for-iam-console-access (p. 163)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.57	A financial institution shall periodically review and adapt its password practices to enhance resilience against evolving attacks. This includes the effective and secure generation of passwords. There must be appropriate controls in place to check the strength of the passwords created.	<a href="#">iam-password-policy (p. 154)</a>	The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. To help protect credentials, this rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
10.58	Authentication methods that depend on more than one factor typically are more difficult to compromise than a single factor system. In view of this, financial institutions are encouraged to properly design and implement (especially in high-risk or 'single sign-on' systems) multi-factor authentication (MFA) that are more reliable and provide stronger fraud deterrents.	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
10.58	Authentication methods that depend on more than one factor typically are more difficult to compromise than a single factor system. In view of this, financial institutions are encouraged to properly design and implement (especially in high-risk or 'single sign-on' systems) multi-factor authentication (MFA) that are more reliable and provide stronger fraud deterrents.	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	Control Description	AWS Config Rule	Guidance
10.58	Authentication methods that depend on more than one factor typically are more difficult to compromise than a single factor system. In view of this, financial institutions are encouraged to properly design and implement (especially in high-risk or 'single sign-on' systems) multi-factor authentication (MFA) that are more reliable and provide stronger fraud deterrents.	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
10.58	Authentication methods that depend on more than one factor typically are more difficult to compromise than a single factor system. In view of this, financial institutions are encouraged to properly design and implement (especially in high-risk or 'single sign-on' systems) multi-factor authentication (MFA) that are more reliable and provide stronger fraud deterrents.	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
10.61	A financial institution must ensure— (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	Control Description	AWS Config Rule	Guidance
10.61	A financial institution must ensure— (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
10.61	A financial institution must ensure— (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner.	<a href="#">cw-loggroup-retention-period-check (p. 125)</a>	Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events.
10.61	A financial institution must ensure— (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.

Control ID	Control Description	AWS Config Rule	Guidance
10.61	A financial institution must ensure— (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
10.61	A financial institution must ensure— (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
10.61	A financial institution must ensure— (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.

Control ID	Control Description	AWS Config Rule	Guidance
10.61	A financial institution must ensure— (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
10.61	A financial institution must ensure— (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
10.61	A financial institution must ensure— (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner.	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.

Control ID	Control Description	AWS Config Rule	Guidance
10.61	<p>A financial institution must ensure— (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner.</p>	<p><a href="#">redshift-cluster-configuration-check (p. 170)</a></p>	<p>To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.</p>
10.61	<p>A financial institution must ensure— (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner.</p>	<p><a href="#">iam-group-has-users-check (p. 153)</a></p>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.61	<p>A financial institution must ensure— (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner.</p>	<p><a href="#">iam-password-policy (p. 154)</a></p>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. To help protect credentials, this rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.61	A financial institution must ensure— (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
10.61	A financial institution must ensure— (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
10.61	A financial institution must ensure— (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
10.61	A financial institution must ensure— (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
10.62	In fulfilling the requirement under paragraph 10.61, large financial institutions are required to— (a) deploy an identity access management system to effectively manage and monitor user access to enterprise-wide systems; and (b) deploy automated audit tools to flag any anomalies.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
10.62	In fulfilling the requirement under paragraph 10.61, large financial institutions are required to— (a) deploy an identity access management system to effectively manage and monitor user access to enterprise-wide systems; and (b) deploy automated audit tools to flag any anomalies.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
10.62	<p>In fulfilling the requirement under paragraph 10.61, large financial institutions are required to— (a) deploy an identity access management system to effectively manage and monitor user access to enterprise-wide systems; and (b) deploy automated audit tools to flag any anomalies.</p>	<p><a href="#">securityhub-enabled (p. 186)</a></p>	<p>AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.</p>
10.63	<p>A financial institution must ensure that critical systems are not running on outdated systems with known security vulnerabilities or end-of-life (EOL) technology systems. In this regard, a financial institution must clearly assign responsibilities to identified functions:</p> <ul style="list-style-type: none"> <li>(a) to continuously monitor and implement latest patch releases in a timely manner;</li> <li>and (b) identify critical technology systems that are approaching EOL for further remedial action.</li> </ul>	<p><a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a></p>	<p>An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.</p>

Control ID	Control Description	AWS Config Rule	Guidance
10.63	A financial institution must ensure that critical systems are not running on outdated systems with known security vulnerabilities or end-of-life (EOL) technology systems. In this regard, a financial institution must clearly assign responsibilities to identified functions: (a) to continuously monitor and implement latest patch releases in a timely manner; and (b) identify critical technology systems that are approaching EOL for further remedial action.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
10.63	A financial institution must ensure that critical systems are not running on outdated systems with known security vulnerabilities or end-of-life (EOL) technology systems. In this regard, a financial institution must clearly assign responsibilities to identified functions: (a) to continuously monitor and implement latest patch releases in a timely manner; and (b) identify critical technology systems that are approaching EOL for further remedial action.	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
10.66(a)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
10.66(a)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
10.66(a)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
10.66(a)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
10.66(a)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).

Control ID	Control Description	AWS Config Rule	Guidance
10.66(a)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
10.66(a)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
10.66(a)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
10.66(a)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
10.66(a)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
10.66(a)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
10.66(a)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
10.66(a)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
10.66(a)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.
10.66(a)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.
10.66(a)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
10.66(a)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions	<a href="#">ec2-ebs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
10.66(a)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.
10.66(a)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
10.66(a)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
10.66(a)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
10.66(b)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (b) reliability of services delivered via channels and devices with minimum disruption to services	<a href="#">dynamodb-autoscaling-enabled (p. 128)</a>	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.
10.66(b)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (b) reliability of services delivered via channels and devices with minimum disruption to services	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.

Control ID	Control Description	AWS Config Rule	Guidance
10.66(b)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (b) reliability of services delivered via channels and devices with minimum disruption to services	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
10.66(b)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (b) reliability of services delivered via channels and devices with minimum disruption to services	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.

Control ID	Control Description	AWS Config Rule	Guidance
10.66(b)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (b) reliability of services delivered via channels and devices with minimum disruption to services	<a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a>	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.
10.66(b)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (b) reliability of services delivered via channels and devices with minimum disruption to services	<a href="#">rds-instance-deletion-protection-enabled (p. 166)</a>	Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
10.66(d)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.

Control ID	Control Description	AWS Config Rule	Guidance
10.66(d)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions	<a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a>	The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.
10.66(d)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
10.66(d)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	Control Description	AWS Config Rule	Guidance
10.66(d)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
10.66(d)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.

Control ID	Control Description	AWS Config Rule	Guidance
10.66(d)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions	<a href="#">dynamodb-throughput-limit-check (p. 130)</a>	Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set <code>accountRCUThresholdPercentage</code> (Config Default: 80) and <code>accountWCUThresholdPercentage</code> (Config Default: 80) parameters. The actual values should reflect your organization's policies.
10.66(d)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions	<a href="#">ec2-instance-detailed-monitoring-enabled (p. 132)</a>	Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance.

Control ID	Control Description	AWS Config Rule	Guidance
10.66(d)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
10.66(d)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
10.66(d)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions	<a href="#">lambda-dlq-check (p. 161)</a>	Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed.

Control ID	Control Description	AWS Config Rule	Guidance
10.66(d)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
10.66(d)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions	<a href="#">rds-enhanced-monitoring-enabled (p. 165)</a>	Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics.

Control ID	Control Description	AWS Config Rule	Guidance
10.66(d)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
10.66(d)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
10.66(d)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
10.66(d)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
10.66(d)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.

Control ID	Control Description	AWS Config Rule	Guidance
10.66(d)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
10.66(e)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (e) ability to identify and revert to the recovery point prior to incident or service disruption	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.
10.66(e)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (e) ability to identify and revert to the recovery point prior to incident or service disruption	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.

Control ID	Control Description	AWS Config Rule	Guidance
10.66(e)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (e) ability to identify and revert to the recovery point prior to incident or service disruption	<a href="#">ebs-optimized-instance (p. 131)</a>	An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance.
10.66(e)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (e) ability to identify and revert to the recovery point prior to incident or service disruption	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
10.66(e)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (e) ability to identify and revert to the recovery point prior to incident or service disruption	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.

Control ID	Control Description	AWS Config Rule	Guidance
10.66(e)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (e) ability to identify and revert to the recovery point prior to incident or service disruption	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.
10.66(e)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (e) ability to identify and revert to the recovery point prior to incident or service disruption	<a href="#">dynamodb-in-backup-plan (p. 128)</a>	To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
10.66(e)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (e) ability to identify and revert to the recovery point prior to incident or service disruption	<a href="#">ebs-in-backup-plan (p. 130)</a>	To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	Control Description	AWS Config Rule	Guidance
10.66(e)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (e) ability to identify and revert to the recovery point prior to incident or service disruption	<a href="#">efs-in-backup-plan (p. 139)</a>	To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
10.66(e)	A financial institution must implement robust technology security controls in providing digital services which assure the following: (e) ability to identify and revert to the recovery point prior to incident or service disruption	<a href="#">rds-in-backup-plan (p. 167)</a>	To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
11.7	A financial institution must deploy effective tools to support the continuous and proactive monitoring and timely detection of anomalous activities in its technology infrastructure. The scope of monitoring must cover all critical systems including the supporting infrastructure.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
11.7	<p>A financial institution must deploy effective tools to support the continuous and proactive monitoring and timely detection of anomalous activities in its technology infrastructure. The scope of monitoring must cover all critical systems including the supporting infrastructure.</p>	<p><a href="#">securityhub-enabled (p. 186)</a></p>	<p>AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.</p>
11.7(c)(f)	<p>The SOC must be able to perform the following functions: (c) vulnerability management; (f) provision of situational awareness to detect adversaries and threats including threat intelligence analysis and operations, and monitoring indicators of compromise (IOC). This includes advanced behavioural analysis to detect signature-less and file-less malware and to identify anomalies that may pose security threats including at endpoints and network layers.</p>	<p><a href="#">guardduty-enabled-centralized (p. 152)</a></p>	<p>Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.7(c)(f)	<p>The SOC must be able to perform the following functions:</p> <ul style="list-style-type: none"> <li>(c) vulnerability management;</li> <li>(f) provision of situational awareness to detect adversaries and threats including threat intelligence analysis and operations, and monitoring indicators of compromise (IOC).</li> </ul> <p>This includes advanced behavioural analysis to detect signature-less and file-less malware and to identify anomalies that may pose security threats including at endpoints and network layers.</p>	<p><a href="#">guardduty-non-archived-findings (p. 152)</a></p>	<p>Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.</p>
11.7(c)(f)	<p>The SOC must be able to perform the following functions:</p> <ul style="list-style-type: none"> <li>(c) vulnerability management;</li> <li>(f) provision of situational awareness to detect adversaries and threats including threat intelligence analysis and operations, and monitoring indicators of compromise (IOC).</li> </ul> <p>This includes advanced behavioural analysis to detect signature-less and file-less malware and to identify anomalies that may pose security threats including at endpoints and network layers.</p>	<p><a href="#">securityhub-enabled (p. 186)</a></p>	<p>AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.8	A financial institution must ensure that its cybersecurity operations continuously prevent and detect any potential compromise of its security controls or weakening of its security posture. For large financial institutions, this must include performing a quarterly vulnerability assessment of external and internal network components that support all critical systems.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
11.8	A financial institution must ensure that its cybersecurity operations continuously prevent and detect any potential compromise of its security controls or weakening of its security posture. For large financial institutions, this must include performing a quarterly vulnerability assessment of external and internal network components that support all critical systems.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
Appendix 5.1	Conduct periodic review on the configuration and rules settings for all security devices. Use automated tools to review and monitor changes to configuration and rules settings. - Appendix 5. Control Measures on Cybersecurity	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
Appendix 5.1	Conduct periodic review on the configuration and rules settings for all security devices. Use automated tools to review and monitor changes to configuration and rules settings. - Appendix 5. Control Measures on Cybersecurity	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
Appendix 5.5(b)	Ensure security controls for server-to-server external network connections include the following: (b) use of secure tunnels such as Transport Layer Security (TLS) and Virtual Private Network (VPN) IPSec	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
Appendix 5.5(b)	Ensure security controls for server-to-server external network connections include the following: (b) use of secure tunnels such as Transport Layer Security (TLS) and Virtual Private Network (VPN) IPSec	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
Appendix 5.5(b)	Ensure security controls for server-to-server external network connections include the following: (b) use of secure tunnels such as Transport Layer Security (TLS) and Virtual Private Network (VPN) IPSec	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
Appendix 5.5(b)	Ensure security controls for server-to-server external network connections include the following: (b) use of secure tunnels such as Transport Layer Security (TLS) and Virtual Private Network (VPN) IPSec	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
Appendix 5.5(b)	Ensure security controls for server-to-server external network connections include the following: (b) use of secure tunnels such as Transport Layer Security (TLS) and Virtual Private Network (VPN) IPSec	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
Appendix 5.5(b)	Ensure security controls for server-to-server external network connections include the following: (b) use of secure tunnels such as Transport Layer Security (TLS) and Virtual Private Network (VPN) IPSec	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
Appendix 5.5(c)	Ensure security controls for server-to-server external network connections include the following: (c) deploying staging servers with adequate perimeter defences and protection such as firewall, IPS and antivirus.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
Appendix 5.5(c)	Ensure security controls for server-to-server external network connections include the following: (c) deploying staging servers with adequate perimeter defences and protection such as firewall, IPS and antivirus.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
Appendix 5.5(c)	Ensure security controls for server-to-server external network connections include the following: (c) deploying staging servers with adequate perimeter defences and protection such as firewall, IPS and antivirus.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
Appendix 5.5(c)	Ensure security controls for server-to-server external network connections include the following: (c) deploying staging servers with adequate perimeter defences and protection such as firewall, IPS and antivirus.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
Appendix 5.5(c)	Ensure security controls for server-to-server external network connections include the following: (c) deploying staging servers with adequate perimeter defences and protection such as firewall, IPS and antivirus.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.

Control ID	Control Description	AWS Config Rule	Guidance
Appendix 5.6	Ensure security controls for remote access to server include the following: (a) restrict access to only hardened and locked down end-point devices; (b) use secure tunnels such as TLS and VPN IPsec; (c) deploy 'gateway' server with adequate perimeter defences and protection such as firewall, IPS and antivirus; and (d) close relevant ports immediately upon expiry of remote access.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
Appendix 5.6	Ensure security controls for remote access to server include the following: (a) restrict access to only hardened and locked down end-point devices; (b) use secure tunnels such as TLS and VPN IPsec; (c) deploy 'gateway' server with adequate perimeter defences and protection such as firewall, IPS and antivirus; and (d) close relevant ports immediately upon expiry of remote access.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
Appendix 5.6	Ensure security controls for remote access to server include the following: (a) restrict access to only hardened and locked down end-point devices; (b) use secure tunnels such as TLS and VPN IPsec; (c) deploy 'gateway' server with adequate perimeter defences and protection such as firewall, IPS and antivirus; and (d) close relevant ports immediately upon expiry of remote access.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
Appendix 5.6	Ensure security controls for remote access to server include the following: (a) restrict access to only hardened and locked down end-point devices; (b) use secure tunnels such as TLS and VPN IPsec; (c) deploy 'gateway' server with adequate perimeter defences and protection such as firewall, IPS and antivirus; and (d) close relevant ports immediately upon expiry of remote access.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.

Control ID	Control Description	AWS Config Rule	Guidance
Appendix 5.6	Ensure security controls for remote access to server include the following: (a) restrict access to only hardened and locked down end-point devices; (b) use secure tunnels such as TLS and VPN IPsec; (c) deploy 'gateway' server with adequate perimeter defences and protection such as firewall, IPS and antivirus; and (d) close relevant ports immediately upon expiry of remote access.	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
Appendix 5.6	Ensure security controls for remote access to server include the following: (a) restrict access to only hardened and locked down end-point devices; (b) use secure tunnels such as TLS and VPN IPsec; (c) deploy 'gateway' server with adequate perimeter defences and protection such as firewall, IPS and antivirus; and (d) close relevant ports immediately upon expiry of remote access.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
Appendix 5.6	Ensure security controls for remote access to server include the following: (a) restrict access to only hardened and locked down end-point devices; (b) use secure tunnels such as TLS and VPN IPsec; (c) deploy 'gateway' server with adequate perimeter defences and protection such as firewall, IPS and antivirus; and (d) close relevant ports immediately upon expiry of remote access.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
Appendix 5.6	Ensure security controls for remote access to server include the following: (a) restrict access to only hardened and locked down end-point devices; (b) use secure tunnels such as TLS and VPN IPsec; (c) deploy 'gateway' server with adequate perimeter defences and protection such as firewall, IPS and antivirus; and (d) close relevant ports immediately upon expiry of remote access.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.

## Template

The template is available on GitHub: [Operational Best Practices for BNM RMIT](#).

# Operational Best Practices for CIS AWS Foundations Benchmark v1.3 Level 1

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Center for Internet Security (CIS) Amazon Web Services Foundation v1.3 Level 1 and AWS managed Config rules/AWS Config Process Checks. Each Config rule applies to a specific AWS resource, and relates to one or more CIS Amazon Web Services Foundation v1.3 Level 1 controls. A CIS Amazon Web Services Foundation v1.3 Level 1 control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

For more information about process checks, see [AWS Config Process Checks Within a Conformance Pack \(p. 222\)](#).

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

Control ID	AWS Config Rule	Guidance
1.1	account-contact-details-configured (Process Check)	Ensure the contact email and telephone number for AWS accounts are current and map to more than one individual in your organization. Within the My Account section of the console ensure correct information is specified in the Contact Information section. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>
1.2	account-security-contact-configured (Process Check)	Ensure the contact email and telephone number for the your organizations security team are current. Within the My Account section of the AWS Management Console ensure the correct information is specified in the Security section. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>
1.3	account-security-questions-configured (Process Check)	Ensure the security questions that can be used to authenticate individuals calling AWS customer service for support are configured. Within the My Account section of the AWS Management Console ensure three security challenge questions are configured.

Control ID	AWS Config Rule	Guidance
		<p>For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a></p>
1.4	<a href="#">iam-root-access-key-check (p. 157)</a>	<p>Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.</p>
1.5	<a href="#">root-account-mfa-enabled (p. 175)</a>	<p>Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.</p>
1.7	<a href="#">root-account-regular-use (Process Check)</a>	<p>Ensure the use of the root account is avoided for everyday tasks. Within IAM, run a credential report to examine when the root user was last used. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a></p>

Control ID	AWS Config Rule	Guidance
1.8	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundational Security Best Practices standard for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	AWS Config Rule	Guidance
1.9	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundational Security Best Practices standard for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>
1.10	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	<p>Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.</p>

Control ID	AWS Config Rule	Guidance
1.11	iam-user-console-and-api-access-at-creation (Process Check)	Ensure access keys are not setup during the initial user setup for all IAM users that have a console password. For all IAM users with console access, compare the user 'Creation time` to the Access Key `Created` date. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>
1.12	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies.
1.13	iam-user-single-access-key (Process Check)	Ensure there is only one active access key available for any single IAM user. For all IAM users check that there is only one active key used within the Security Credentials tab for each user within IAM. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>

Control ID	AWS Config Rule	Guidance
1.14	<a href="#">access-keys-rotated (p. 107)</a>	<p>The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.</p>
1.15	<a href="#">iam-user-no-policies-check (p. 158)</a>	<p>This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.</p>
1.15	<a href="#">iam-no-inline-policy-check (p. 154)</a>	<p>Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.</p>
1.15	<a href="#">iam-user-group-membership-check (p. 157)</a>	<p>AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.</p>

Control ID	AWS Config Rule	Guidance
1.16	<a href="#">iam-policy-no-statements-with-admin-access</a> (p. 156)	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
1.17	iam-support-role-created (Process Check)	Ensure a support role has been created to manage incidents with AWS Support. Check that the AWSSupportAccess policy is attached to an IAM role. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>
1.19	iam-expired-certificates (Process Check)	Ensure that all the expired SSL/TLS certificates stored in IAM are removed. From the command line with the installed AWS CLI run the 'aws iam list-server-certificates' command and determine if there are any expired server certificates. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>

Control ID	AWS Config Rule	Guidance
1.20	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.
1.21	<code>iam-access-analyzer-enabled</code> (Process Check)	Ensure that IAM Access Analyzer is enabled. Within the IAM section of the console, select Access Analyzer and ensure that the STATUS is set to Active. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>
2.1.1	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
2.2.1	<a href="#">ec2-efs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
2.2.1	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
3.1	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
3.3	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
3.3	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	AWS Config Rule	Guidance
3.3	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.
3.3	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
3.4	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
3.5	<code>config-enabled-all-regions</code> (Process Check)	Ensure AWS Config is enabled in all AWS Regions. Within the AWS Config section of the console, for each Region enabled ensure the AWS Config recorder is configured correctly. Ensure recording of global AWS resources is enabled at least in one Region. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>

Control ID	AWS Config Rule	Guidance
3.6	<a href="#">s3-bucket-logging-enabled</a> (p. 177)	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
4.1	alarm-unauthorized-api-calls (Process Check)	Ensure a log metric filter and an alarm exists for unauthorized API calls. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>
4.2	alarm-sign-in-without-mfa (Process Check)	Ensure a log metric filter and an alarm exists for AWS Management Console sign-in without Multi-Factor Authentication (MFA). For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>
4.3	alarm-root-account-use (Process Check)	Ensure a log metric filter and an alarm exists for usage of the root account. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>

Control ID	AWS Config Rule	Guidance
4.4	alarm-iam-policy-change (Process Check)	Ensure a log metric filter and an alarm exists for IAM policy changes. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>
4.5	alarm-cloudtrail-config-change (Process Check)	Ensure a log metric filter and an alarm exists for AWS CloudTrail configuration changes. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>
4.8	alarm-s3-bucket-policy-change (Process Check)	Ensure a log metric filter and an alarm exists for Amazon S3 bucket policy changes. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>
4.12	alarm-vpc-network-gateway-change (Process Check)	Ensure a log metric filter and an alarm exists for changes to network gateways. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>

Control ID	AWS Config Rule	Guidance
4.13	alarm-vpc-route-table-change (Process Check)	Ensure a log metric filter and an alarm exists for route table changes. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>
4.14	alarm-vpc-change (Process Check)	Ensure a log metric filter and an alarm exists for Amazon Virtual Private Cloud (VPC) changes. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>
4.15	alarm-organizations-change (Process Check)	Ensure a log metric filter and an alarm exists for AWS Organizations changes. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>
5.1	vpc-networkacl-open-admin-ports (Process Check)	Ensure no network ACLs allow public ingress to the remote server administration ports. Within the VPC section of the console, ensure there are network ACLs with a source of '0.0.0.0/0' with allowing ports or port ranges including remote server admin ports. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>

Control ID	AWS Config Rule	Guidance
5.2	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

## Template

The template is available on GitHub: [Operational Best Practices for CIS AWS Foundations Benchmark v1.3 Level 1](#).

# Operational Best Practices for CIS AWS Foundations Benchmark v1.3 Level 2

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Center for Internet Security (CIS) Amazon Web Services Foundation v1.3 Level 2 and AWS managed Config rules/AWS Config Process Checks. Each Config rule applies to a specific AWS resource, and relates to one or more CIS Amazon Web Services Foundation v1.3 Level 2 controls. A CIS Amazon Web Services Foundation v1.3 Level 2 control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

For more information about process checks, see [AWS Config Process Checks Within a Conformance Pack \(p. 222\)](#).

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

Control ID	AWS Config Rule	Guidance
1.1	account-contact-details-configured (Process Check)	Ensure the contact email and telephone number for AWS accounts are current and map to more than one individual in your organization. Within the My Account section of

Control ID	AWS Config Rule	Guidance
		<p>the console ensure correct information is specified in the Contact Information section. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a></p>
1.2	account-security-contact-configured (Process Check)	<p>Ensure the contact email and telephone number for the your organizations security team are current. Within the My Account section of the AWS Management Console ensure the correct information is specified in the Security section. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a></p>
1.3	account-security-questions-configured (Process Check)	<p>Ensure the security questions that can be used to authenticate individuals calling AWS customer service for support are configured. Within the My Account section of the AWS Management Console ensure three security challenge questions are configured. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a></p>

Control ID	AWS Config Rule	Guidance
1.4	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
1.5	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
1.6	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
1.7	root-account-regular-use (Process Check)	Ensure the use of the root account is avoided for everyday tasks. Within IAM, run a credential report to examine when the root user was last used. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>

Control ID	AWS Config Rule	Guidance
1.8	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundational Security Best Practices standard for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	AWS Config Rule	Guidance
1.9	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundational Security Best Practices standard for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>
1.10	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	<p>Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.</p>

Control ID	AWS Config Rule	Guidance
1.11	iam-user-console-and-api-access-at-creation (Process Check)	Ensure access keys are not setup during the initial user setup for all IAM users that have a console password. For all IAM users with console access, compare the user 'Creation time` to the Access Key `Created` date. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>
1.12	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies.
1.13	iam-user-single-access-key (Process Check)	Ensure there is only one active access key available for any single IAM user. For all IAM users check that there is only one active key used within the Security Credentials tab for each user within IAM. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>

Control ID	AWS Config Rule	Guidance
1.14	<a href="#">access-keys-rotated (p. 107)</a>	The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.
1.15	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
1.15	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
1.15	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	AWS Config Rule	Guidance
1.16	<a href="#">iam-policy-no-statements-with-admin-access</a> (p. 156)	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
1.17	iam-support-role-created (Process Check)	Ensure a support role has been created to manage incidents with AWS Support. Check that the AWSSupportAccess policy is attached to an IAM role. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>
1.18	ec2-instance-role-assigned (Process Check)	For instances that are known to perform AWS actions, ensure that they belong to an instance role that has the necessary permissions. Within the EC2 section of the AWS Management Console select the instance and check that the IAM role field is populated. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>

Control ID	AWS Config Rule	Guidance
1.19	iam-expired-certificates (Process Check)	<p>Ensure that all the expired SSL/TLS certificates stored in IAM are removed. From the command line with the installed AWS CLI run the 'aws iam list-server-certificates' command and determine if there are any expired server certificates. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a></p>
1.20	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.</p>
1.21	iam-access-analyzer-enabled (Process Check)	<p>Ensure that IAM Access Analyzer is enabled. Within the IAM section of the console, select Access Analyzer and ensure that the STATUS is set to Active. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a></p>

Control ID	AWS Config Rule	Guidance
1.22	iam-central-user-management (Process Check)	Ensure IAM users are managed centrally via the identity federation or AWS Organizations for multi-account environments. Within the IAM section of the AWS Management Console, confirm that no IAM users representing individuals are present. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>
2.1.1	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
2.1.2	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
2.2.1	<a href="#">ec2-efs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
2.2.1	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.

Control ID	AWS Config Rule	Guidance
3.1	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	<p>AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.</p>
3.2	<a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a>	<p>Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.</p>
3.3	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	<p>Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.</p>
3.3	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	<p>Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.</p>

Control ID	AWS Config Rule	Guidance
3.3	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.
3.3	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
3.4	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
3.5	<code>config-enabled-all-regions</code> (Process Check)	Ensure AWS Config is enabled in all AWS Regions. Within the AWS Config section of the console, for each Region enabled ensure the AWS Config recorder is configured correctly. Ensure recording of global AWS resources is enabled at least in one Region. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>

Control ID	AWS Config Rule	Guidance
3.6	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
3.7	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
3.8	<a href="#">cmk-backing-key-rotation-enabled (p. 123)</a>	Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period.
3.9	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
3.10	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
3.11	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.

Control ID	AWS Config Rule	Guidance
4.1	alarm-unauthorized-api-calls (Process Check)	Ensure a log metric filter and an alarm exists for unauthorized API calls. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>
4.2	alarm-sign-in-without-mfa (Process Check)	Ensure a log metric filter and an alarm exists for AWS Management Console sign-in without Multi-Factor Authentication (MFA). For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>
4.3	alarm-root-account-use (Process Check)	Ensure a log metric filter and an alarm exists for usage of the root account. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>
4.4	alarm-iam-policy-change (Process Check)	Ensure a log metric filter and an alarm exists for IAM policy changes. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>

Control ID	AWS Config Rule	Guidance
4.5	alarm-cloudtrail-config-change (Process Check)	Ensure a log metric filter and an alarm exists for AWS CloudTrail configuration changes. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>
4.6	alarm-console-auth-failures (Process Check)	Ensure a log metric filter and an alarm exists for AWS Management Console authentication failures. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>
4.7	alarm-kms-disable-or-delete-cmk (Process Check)	Ensure a log metric filter and an alarm exists for disabling or scheduled deletion of customer created CMKs. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>
4.8	alarm-s3-bucket-policy-change (Process Check)	Ensure a log metric filter and an alarm exists for Amazon S3 bucket policy changes. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>

Control ID	AWS Config Rule	Guidance
4.9	alarm-aws-config-change (Process Check)	Ensure a log metric filter and an alarm exists for AWS Config configuration changes. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>
4.10	alarm-vpc-security-group-change (Process Check)	Ensure a log metric filter and an alarm exists for security group changes. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>
4.11	alarm-vpc-nacl-change (Process Check)	Ensure a log metric filter and an alarm exists for changes to Network Access Control Lists (NACL). For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>
4.12	alarm-vpc-network-gateway-change (Process Check)	Ensure a log metric filter and an alarm exists for changes to network gateways. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>

Control ID	AWS Config Rule	Guidance
4.13	alarm-vpc-route-table-change (Process Check)	Ensure a log metric filter and an alarm exists for route table changes. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>
4.14	alarm-vpc-change (Process Check)	Ensure a log metric filter and an alarm exists for Amazon Virtual Private Cloud (VPC) changes. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>
4.15	alarm-organizations-change (Process Check)	Ensure a log metric filter and an alarm exists for AWS Organizations changes. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>
5.1	vpc-networkacl-open-admin-ports (Process Check)	Ensure no network ACLs allow public ingress to the remote server administration ports. Within the VPC section of the console, ensure there are network ACLs with a source of '0.0.0.0/0' with allowing ports or port ranges including remote server admin ports. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>

Control ID	AWS Config Rule	Guidance
5.2	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
5.3	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
5.4	<a href="#">vpc-networkacl-open-admin-ports (Process Check)</a>	Ensure the routing tables for Amazon VPC peering are "least access". Within the VPC section of the console, examine the route table entries to ensure that the least number of subnets or hosts are required to accomplish the purpose for peering are routable. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.3.0 document available at <a href="https://www.cisecurity.org/benchmark/amazon_web_services/">https://www.cisecurity.org/benchmark/amazon_web_services/</a>

## Template

The template is available on GitHub: [Operational Best Practices for CIS AWS Foundations Benchmark v1.3 Level 2](#).

## Operational Best Practices for CIS Top 20

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Center for Internet Security (CIS) Top 20 Critical Security Controls and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more CIS Top 20 controls. A CIS Top 20 control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This Conformance Pack was validated by AWS Security Assurance Services LLC (AWS SAS), which is a team of Payment Card Industry Qualified Security Assessors (QSAs), HITRUST Certified Common Security Framework Practitioners (CCSFPs), and compliance professionals certified to provide guidance and assessments for various industry frameworks. AWS SAS professionals designed this Conformance Pack to enable a customer to align to a subset of the CIS Top 20.

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

Control ID	AWS Config Rule	Guidance
CIS.2	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
CIS.2	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
CIS.2	<a href="#">ec2-security-group-attached-to-eni (p. 137)</a>	This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment.

Control ID	AWS Config Rule	Guidance
CIS.2	<a href="#">ec2-stopped-instance (p. 137)</a>	Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards.
CIS.2	<a href="#">ec2-volume-inuse-check (p. 137)</a>	This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality.
CIS.2	<a href="#">eip-attached (p. 139)</a>	This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment.
CIS.3	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	AWS Config Rule	Guidance
CIS.3	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.
CIS.3	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
CIS.4	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
CIS.4	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	AWS Config Rule	Guidance
CIS.4	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
CIS.4	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
CIS.4	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
CIS.4	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	AWS Config Rule	Guidance
CIS.5	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
CIS.5	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
CIS.5	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.

Control ID	AWS Config Rule	Guidance
CIS.5	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
CIS.5	<a href="#">redshift-cluster-maintenancesettings-check (p. 171)</a>	This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the <code>allowVersionUpgrade</code> . The default is true. It also lets you optionally set the <code>preferredMaintenanceWindow</code> (the default is sat:16:00-sat:16:30), and the <code>automatedSnapshotRetentionPeriod</code> (the default is 1). The actual values should reflect your organization's policies.
CIS.6	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
CIS.6	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	AWS Config Rule	Guidance
CIS.6	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
CIS.6	<a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a>	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.
CIS.6	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
CIS.6	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment.

Control ID	AWS Config Rule	Guidance
CIS.6	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
CIS.6	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
CIS.6	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.

Control ID	AWS Config Rule	Guidance
CIS.6	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	<p>AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.</p>
CIS.6	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	<p>To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.</p>
CIS.6	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	<p>Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.</p>

Control ID	AWS Config Rule	Guidance
CIS.6	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
CIS.6	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
CIS.8	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
CIS.9	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
CIS.9	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
CIS.9	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
CIS.9	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
CIS.9	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
CIS.9	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	AWS Config Rule	Guidance
CIS.9	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
CIS.9	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
CIS.9	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	AWS Config Rule	Guidance
CIS.9	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
CIS.9	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
CIS.9	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
CIS.9	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
CIS.9	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
CIS.9	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
CIS.9	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
CIS.9	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	AWS Config Rule	Guidance
CIS.9	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
CIS.9	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
CIS.9	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
CIS.10	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.
CIS.10	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.

Control ID	AWS Config Rule	Guidance
CIS.10	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
CIS.10	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
CIS.10	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.
CIS.11	<a href="#">ec2-security-group-attached-to-eni (p. 137)</a>	This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment.

Control ID	AWS Config Rule	Guidance
CIS.11	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
CIS.11	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
CIS.11	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
CIS.11	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.

Control ID	AWS Config Rule	Guidance
CIS.12	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
CIS.12	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
CIS.12	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
CIS.12	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
CIS.12	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
CIS.12	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
CIS.12	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
CIS.12	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
CIS.12	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.

Control ID	AWS Config Rule	Guidance
CIS.12	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
CIS.12	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
CIS.12	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
CIS.12	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
CIS.12	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
CIS.12	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
CIS.12	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
CIS.12	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	AWS Config Rule	Guidance
CIS.12	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
CIS.12	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
CIS.12	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
CIS.12	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	AWS Config Rule	Guidance
CIS.12	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
CIS.13	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.
CIS.13	<a href="#">alb-http-to-https-redirection-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
CIS.13	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
CIS.13	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
CIS.13	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.

Control ID	AWS Config Rule	Guidance
CIS.13	<a href="#">ec2-efs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
CIS.13	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
CIS.13	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
CIS.13	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
CIS.13	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
CIS.13	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	AWS Config Rule	Guidance
CIS.13	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.
CIS.13	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.
CIS.13	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.
CIS.13	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
CIS.13	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
CIS.13	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.
CIS.13	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
CIS.13	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
CIS.13	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.
CIS.13	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
CIS.13	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.
CIS.14	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.
CIS.14	<a href="#">alb-http-to-https-redirection-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
CIS.14	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
CIS.14	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
CIS.14	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.

Control ID	AWS Config Rule	Guidance
CIS.14	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
CIS.14	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
CIS.14	<a href="#">ec2-ebs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
CIS.14	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
CIS.14	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
CIS.14	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
CIS.14	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.

Control ID	AWS Config Rule	Guidance
CIS.14	<a href="#">emr-kerberos-enabled (p. 145)</a>	<p>The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.</p>
CIS.14	<a href="#">encrypted-volumes (p. 146)</a>	<p>Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.</p>
CIS.14	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	<p>To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.</p>
CIS.14	<a href="#">rds-instance-public-access-check (p. 166)</a>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.</p>

Control ID	AWS Config Rule	Guidance
CIS.14	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.
CIS.14	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
CIS.14	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.
CIS.14	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
CIS.14	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	AWS Config Rule	Guidance
CIS.14	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.
CIS.14	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.
CIS.14	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
CIS.14	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	AWS Config Rule	Guidance
CIS.14	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
CIS.14	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
CIS.14	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
CIS.14	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.
CIS.14	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.
CIS.14	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
CIS.16	<a href="#">access-keys-rotated (p. 107)</a>	<p>The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.</p>
CIS.16	<a href="#">cloudtrail-enabled (p. 121)</a>	<p>AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.</p>
CIS.16	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	<p>Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.</p>

Control ID	AWS Config Rule	Guidance
CIS.16	<a href="#">emr-kerberos-enabled (p. 145)</a>	<p>The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.</p>
CIS.16	<a href="#">guardduty-enabled-centralized (p. 152)</a>	<p>Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.</p>
CIS.16	<a href="#">guardduty-non-archived-findings (p. 152)</a>	<p>Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.</p>

Control ID	AWS Config Rule	Guidance
CIS.16	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>
CIS.16	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.</p>

Control ID	AWS Config Rule	Guidance
CIS.16	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
CIS.16	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
CIS.16	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
CIS.16	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	AWS Config Rule	Guidance
CIS.16	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.
CIS.16	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
CIS.16	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
CIS.16	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	AWS Config Rule	Guidance
CIS.16	<a href="#">secretsmanager-rotation-enabled-check (p. 183)</a>	This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised.
CIS.16	<a href="#">secretsmanager-scheduled-rotation-success-check (p. 184)</a>	This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised.
CIS.16	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
CIS.18	<a href="#">codebuild-project-envvar-awscred-check (p. 123)</a>	Ensure authentication credentials <code>AWS_ACCESS_KEY_ID</code> and <code>AWS_SECRET_ACCESS_KEY</code> do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access.

Control ID	AWS Config Rule	Guidance
CIS.18	<a href="#">codebuild-project-source-repo-url-check (p. 123)</a>	Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, user name and password within AWS Codebuild project environments. Use OAuth instead of personal access tokens or a user name and password to grant authorization for accessing GitHub or Bitbucket repositories.
CIS.19	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
CIS.19	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.
CIS.19	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	AWS Config Rule	Guidance
CIS.2	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

## Template

The template is available on GitHub: [Operational Best Practices for CIS Top 20](#).

## Operational Best Practices for CMMC Level 1

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Cybersecurity Maturity Model Certification (CMMC) Level 1 and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more CMMC Level 1 controls. A CMMC Level 1 control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This Conformance Pack was validated by AWS Security Assurance Services LLC (AWS SAS), which is a team of Payment Card Industry Qualified Security Assessors (QSAs), HITRUST Certified Common Security Framework Practitioners (CCSFPs), and compliance professionals certified to provide guidance and assessments for various industry frameworks. AWS SAS professionals designed this Conformance Pack to enable a customer to align to a subset of the CMMC Level 1.

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by

Control ID	Control Description	AWS Config Rule	Guidance
			ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">ec2-imsdv2-check (p. 132)</a>	Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">alb-waf-enabled (p. 109)</a>	Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.

Control ID	Control Description	AWS Config Rule	Guidance
IA.1.076	Identify information system users, processes acting on behalf of users, or devices.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
IA.1.076	Identify information system users, processes acting on behalf of users, or devices.	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.

Control ID	Control Description	AWS Config Rule	Guidance
IA.1.076	Identify information system users, processes acting on behalf of users, or devices.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
IA.1.076	Identify information system users, processes acting on behalf of users, or devices.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
IA.1.076	Identify information system users, processes acting on behalf of users, or devices.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
IA.1.076	Identify information system users, processes acting on behalf of users, or devices.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
IA.1.077	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
IA.1.077	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
IA.1.077	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.

Control ID	Control Description	AWS Config Rule	Guidance
IA.1.077	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
IA.1.077	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
IA.1.077	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
SC.1.176	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.

Control ID	Control Description	AWS Config Rule	Guidance
SI.1.210	Identify, report, and correct information and information system flaws in a timely manner.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
SI.1.210	Identify, report, and correct information and information system flaws in a timely manner.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
SI.1.210	Identify, report, and correct information and information system flaws in a timely manner.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
SI.1.211	Provide protection from malicious code at appropriate locations within organizational information systems.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
SI.1.211	Provide protection from malicious code at appropriate locations within organizational information systems.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

## Template

The template is available on GitHub: [Operational Best Practices for CMMC Level 1](#).

## Operational Best Practices for CMMC Level 2

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Cybersecurity Maturity Model Certification (CMMC) Level 2 and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more CMMC Level 2 controls. A CMMC Level 2 control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This Conformance Pack was validated by AWS Security Assurance Services LLC (AWS SAS), which is a team of Payment Card Industry Qualified Security Assessors (QSAs), HITRUST Certified Common Security Framework Practitioners (CCSFPs), and compliance professionals certified to provide guidance and assessments for various industry frameworks. AWS SAS professionals designed this Conformance Pack to enable a customer to align to a subset of the CMMC Level 2.

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users,	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you

Control ID	Control Description	AWS Config Rule	Guidance
	processes acting on behalf of authorized users, or devices (including other information systems).		incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">ec2-imsdv2-check (p. 132)</a>	Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">alb-waf-enabled (p. 109)</a>	Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.

Control ID	Control Description	AWS Config Rule	Guidance
IA.1.076	Identify information system users, processes acting on behalf of users, or devices.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
IA.1.076	Identify information system users, processes acting on behalf of users, or devices.	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.

Control ID	Control Description	AWS Config Rule	Guidance
IA.1.076	Identify information system users, processes acting on behalf of users, or devices.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
IA.1.076	Identify information system users, processes acting on behalf of users, or devices.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
IA.1.076	Identify information system users, processes acting on behalf of users, or devices.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
IA.1.076	Identify information system users, processes acting on behalf of users, or devices.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
IA.1.077	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
IA.1.077	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
IA.1.077	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.

Control ID	Control Description	AWS Config Rule	Guidance
IA.1.077	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
IA.1.077	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
IA.1.077	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
SC.1.176	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.

Control ID	Control Description	AWS Config Rule	Guidance
SI.1.210	Identify, report, and correct information and information system flaws in a timely manner.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
SI.1.210	Identify, report, and correct information and information system flaws in a timely manner.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
SI.1.210	Identify, report, and correct information and information system flaws in a timely manner.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
SI.1.211	Provide protection from malicious code at appropriate locations within organizational information systems.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
SI.1.211	Provide protection from malicious code at appropriate locations within organizational information systems.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">ec2-imdsv2-check (p. 132)</a>	Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.008	Use non-privileged accounts or roles when accessing nonsecurity functions.	<a href="#">emr-kerberos-enabled (p. 145)</a>	<p>The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.</p>
AC.2.008	Use non-privileged accounts or roles when accessing nonsecurity functions.	<a href="#">iam-group-has-users-check (p. 153)</a>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.008	Use non-privileged accounts or roles when accessing nonsecurity functions.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC.2.008	Use non-privileged accounts or roles when accessing nonsecurity functions.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
AC.2.008	Use non-privileged accounts or roles when accessing nonsecurity functions.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.008	Use non-privileged accounts or roles when accessing nonsecurity functions.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
AC.2.008	Use non-privileged accounts or roles when accessing nonsecurity functions.	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.013	Monitor and control remote access sessions.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
AC.2.013	Monitor and control remote access sessions.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.013	Monitor and control remote access sessions.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
AC.2.013	Monitor and control remote access sessions.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
AU.2.041	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
AU.2.041	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
AU.2.041	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
AU.2.041	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
AU.2.041	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
AU.2.041	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
AU.2.041	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">cw-loggroup-retention-period-check (p. 125)</a>	Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events.
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	<a href="#">ec2-security-group-attached-to-eni (p. 137)</a>	This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment.
CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	<a href="#">ec2-stopped-instance (p. 137)</a>	Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards.
CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	<a href="#">ec2-volume-in-use-check (p. 137)</a>	This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	<a href="#">eip-attached (p. 139)</a>	This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">ec2-volume-inuse-check (p. 137)</a>	This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality.
CM.2.063	Control and monitor user-installed software.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.063	Control and monitor user-installed software.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
CM.2.064	Establish and enforce security configuration settings for information technology products employed in organizational systems.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.064	Establish and enforce security configuration settings for information technology products employed in organizational systems.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
CM.2.064	Establish and enforce security configuration settings for information technology products employed in organizational systems.	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
CM.2.064	Establish and enforce security configuration settings for information technology products employed in organizational systems.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.064	Establish and enforce security configuration settings for information technology products employed in organizational systems.	<a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a>	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.
CM.2.064	Establish and enforce security configuration settings for information technology products employed in organizational systems.	<a href="#">account-part-of-organizations (p. 108)</a>	Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data.
CM.2.064	Establish and enforce security configuration settings for information technology products employed in organizational systems.	<a href="#">cloudtrail-security-trail-enabled (p. 118)</a>	This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.065	Track, review, approve, or disapprove, and log changes to organizational systems.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
CM.2.065	Track, review, approve, or disapprove, and log changes to organizational systems.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.065	Track, review, approve, or disapprove, and log changes to organizational systems.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
CM.2.065	Track, review, approve, or disapprove, and log changes to organizational systems.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.065	Track, review, approve, or disapprove, and log changes to organizational systems.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
CM.2.065	Track, review, approve, or disapprove, and log changes to organizational systems.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.065	Track, review, approve, or disapprove, and log changes to organizational systems.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
IA.2.078	Enforce a minimum password complexity and change of characters when new passwords are created.	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
IA.2.079	Prohibit password reuse for a specified number of generations.	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.

Control ID	Control Description	AWS Config Rule	Guidance
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">ec2-ebs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
IR.2.092	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
IR.2.092	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
IR.2.092	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.
IR.2.092	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	<a href="#">lambda-dlq-check (p. 161)</a>	Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed.
IR.2.092	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
IR.2.093	Detect and report events.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
IR.2.093	Detect and report events.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
IR.2.093	Detect and report events.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
IR.2.093	Detect and report events.	<a href="#">lambda-dlq-check (p. 161)</a>	Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed.
MA.2.113	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.

Control ID	Control Description	AWS Config Rule	Guidance
MA.2.113	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
RE.2.137	Regularly perform and test data backups.	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.
RE.2.137	Regularly perform and test data backups.	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.

Control ID	Control Description	AWS Config Rule	Guidance
RE.2.137	Regularly perform and test data backups.	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
RE.2.137	Regularly perform and test data backups.	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
RE.2.137	Regularly perform and test data backups.	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.

Control ID	Control Description	AWS Config Rule	Guidance
RE.2.137	Regularly perform and test data backups.	<a href="#">dynamodb-in-backup-plan (p. 128)</a>	To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
RE.2.137	Regularly perform and test data backups.	<a href="#">ebs-in-backup-plan (p. 130)</a>	To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
RE.2.137	Regularly perform and test data backups.	<a href="#">efs-in-backup-plan (p. 139)</a>	To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	Control Description	AWS Config Rule	Guidance
RE.2.137	Regularly perform and test data backups.	<a href="#">rds-in-backup-plan (p. 167)</a>	To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
RM.2.142	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.

Control ID	Control Description	AWS Config Rule	Guidance
SI.2.214	Monitor system security alerts and advisories and take action in response.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
SI.2.214	Monitor system security alerts and advisories and take action in response.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
SI.2.214	Monitor system security alerts and advisories and take action in response.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
SI.2.214	Monitor system security alerts and advisories and take action in response.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
SI.2.214	Monitor system security alerts and advisories and take action in response.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
SI.2.216	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
SI.2.216	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
SI.2.216	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
SI.2.216	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	<a href="#">alb-waf-enabled (p. 109)</a>	Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.

Control ID	Control Description	AWS Config Rule	Guidance
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.

Control ID	Control Description	AWS Config Rule	Guidance
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.

## Template

The template is available on GitHub: [Operational Best Practices for CMMC Level 2](#).

## Operational Best Practices for CMMC Level 3

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Cybersecurity Maturity Model Certification (CMMC) Level 3 and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more CMMC Level 3 controls. A CMMC Level 3 control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This Conformance Pack was validated by AWS Security Assurance Services LLC (AWS SAS), which is a team of Payment Card Industry Qualified Security Assessors (QSAs), HITRUST Certified Common Security Framework Practitioners (CSFPs), and compliance professionals certified to provide guidance and assessments for various industry frameworks. AWS SAS professionals designed this Conformance Pack to enable a customer to align to a subset of the CMMC Level 3.

**AWS Region:** Due to tentative guidance provided by the DoD and the CMMC Accreditation Body with respect to FedRAMP reciprocity for CMMC Level 3 - 5, it is recommended that customers use AWS GovCloud (US) regions at this time for any workloads that require compliance with CMMC Level 3 - 5. As such, conformance pack templates for CMMC Levels 3 - 5 are not available within the conformance pack console to avoid confusion. Customers may independently install Config rules that map the tentative guidance for CMMC Level 3-5 (without a conformance pack template) via CloudFormation using the sample YAML file linked within this document.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-password-policy (p. 154)</a>	The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best

Control ID	Control Description	AWS Config Rule	Guidance
			<p>Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">ec2-imsdv2-check (p. 132)</a>	Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
IA.1.076	Identify information system users, processes acting on behalf of users, or devices.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	Control Description	AWS Config Rule	Guidance
IA.1.076	Identify information system users, processes acting on behalf of users, or devices.	<a href="#">emr-kerberos-enabled (p. 145)</a>	<p>The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.</p>

Control ID	Control Description	AWS Config Rule	Guidance
IA.1.076	Identify information system users, processes acting on behalf of users, or devices.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
IA.1.076	Identify information system users, processes acting on behalf of users, or devices.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
IA.1.076	Identify information system users, processes acting on behalf of users, or devices.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
IA.1.076	Identify information system users, processes acting on behalf of users, or devices.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
IA.1.077	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
IA.1.077	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
IA.1.077	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.

Control ID	Control Description	AWS Config Rule	Guidance
IA.1.077	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), and <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">alb-http-to-https-redirection-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.176	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
SI.1.210	Identify, report, and correct information and information system flaws in a timely manner.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
SI.1.210	Identify, report, and correct information and information system flaws in a timely manner.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
SI.1.211	Provide protection from malicious code at appropriate locations within organizational information systems.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">emr-kerberos-enabled (p. 145)</a>	<p>The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.</p>
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">iam-group-has-users-check (p. 153)</a>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">ec2-imsdv2-check (p. 132)</a>	Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.008	Use non-privileged accounts or roles when accessing nonsecurity functions.	<a href="#">emr-kerberos-enabled (p. 145)</a>	<p>The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.</p>
AC.2.008	Use non-privileged accounts or roles when accessing nonsecurity functions.	<a href="#">iam-group-has-users-check (p. 153)</a>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.008	Use non-privileged accounts or roles when accessing nonsecurity functions.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC.2.008	Use non-privileged accounts or roles when accessing nonsecurity functions.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
AC.2.008	Use non-privileged accounts or roles when accessing nonsecurity functions.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.008	Use non-privileged accounts or roles when accessing nonsecurity functions.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
AC.2.008	Use non-privileged accounts or roles when accessing nonsecurity functions.	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.013	Monitor and control remote access sessions.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
AC.2.013	Monitor and control remote access sessions.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
AC.2.013	Monitor and control remote access sessions.	<a href="#">cloud-trail-cloudwatch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
AU.2.041	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
AU.2.041	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
AU.2.041	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
AU.2.041	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
AU.2.041	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
AU.2.041	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
AU.2.041	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">cw-loggroup-retention-period-check (p. 125)</a>	Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events.
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	<a href="#">ec2-security-group-attached-to-eni (p. 137)</a>	This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	<a href="#">ec2-stopped-instance (p. 137)</a>	Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards.
CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	<a href="#">ec2-volume-in-use-check (p. 137)</a>	This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality.
CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	<a href="#">eip-attached (p. 139)</a>	This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">ec2-volume-inuse-check (p. 137)</a>	This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality.
CM.2.063	Control and monitor user-installed software.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.063	Control and monitor user-installed software.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
CM.2.064	Establish and enforce security configuration settings for information technology products employed in organizational systems.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.064	Establish and enforce security configuration settings for information technology products employed in organizational systems.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
CM.2.064	Establish and enforce security configuration settings for information technology products employed in organizational systems.	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
CM.2.064	Establish and enforce security configuration settings for information technology products employed in organizational systems.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.064	Establish and enforce security configuration settings for information technology products employed in organizational systems.	<a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a>	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.
CM.2.064	Establish and enforce security configuration settings for information technology products employed in organizational systems.	<a href="#">account-part-of-organizations (p. 108)</a>	Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data.
CM.2.064	Establish and enforce security configuration settings for information technology products employed in organizational systems.	<a href="#">cloudtrail-security-trail-enabled (p. 118)</a>	This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.065	Track, review, approve, or disapprove, and log changes to organizational systems.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
CM.2.065	Track, review, approve, or disapprove, and log changes to organizational systems.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.065	Track, review, approve, or disapprove, and log changes to organizational systems.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
CM.2.065	Track, review, approve, or disapprove, and log changes to organizational systems.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.065	Track, review, approve, or disapprove, and log changes to organizational systems.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
CM.2.065	Track, review, approve, or disapprove, and log changes to organizational systems.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.065	Track, review, approve, or disapprove, and log changes to organizational systems.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
IA.2.078	Enforce a minimum password complexity and change of characters when new passwords are created.	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
IA.2.079	Prohibit password reuse for a specified number of generations.	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.

Control ID	Control Description	AWS Config Rule	Guidance
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">ec2-ebs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
IR.2.092	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), and <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
IR.2.092	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	<a href="#">lambda-dlq-check (p. 161)</a>	Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed.

Control ID	Control Description	AWS Config Rule	Guidance
IR.2.092	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
IR.2.093	Detect and report events.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.

Control ID	Control Description	AWS Config Rule	Guidance
IR.2.093	Detect and report events.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
IR.2.093	Detect and report events.	<a href="#">lambda-dlq-check (p. 161)</a>	Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed.
MA.2.113	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.

Control ID	Control Description	AWS Config Rule	Guidance
MA.2.113	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
RE.2.137	Regularly perform and test data backups.	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.
RE.2.137	Regularly perform and test data backups.	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.

Control ID	Control Description	AWS Config Rule	Guidance
RE.2.137	Regularly perform and test data backups.	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
RE.2.137	Regularly perform and test data backups.	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
RE.2.137	Regularly perform and test data backups.	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.

Control ID	Control Description	AWS Config Rule	Guidance
RM.2.142	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
SI.2.214	Monitor system security alerts and advisories and take action in response.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.

Control ID	Control Description	AWS Config Rule	Guidance
SI.2.214	Monitor system security alerts and advisories and take action in response.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
SI.2.214	Monitor system security alerts and advisories and take action in response.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
SI.2.214	Monitor system security alerts and advisories and take action in response.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
SI.2.216	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
SI.2.216	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.

Control ID	Control Description	AWS Config Rule	Guidance
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	<p>To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.</p>
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">elb-logging-enabled (p. 144)</a>	<p>Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.

Control ID	Control Description	AWS Config Rule	Guidance
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.

Control ID	Control Description	AWS Config Rule	Guidance
AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.

Control ID	Control Description	AWS Config Rule	Guidance
AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.

Control ID	Control Description	AWS Config Rule	Guidance
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">emr-kerberos-enabled (p. 145)</a>	<p>The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.</p>
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">iam-group-has-users-check (p. 153)</a>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.

Control ID	Control Description	AWS Config Rule	Guidance
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.

Control ID	Control Description	AWS Config Rule	Guidance
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.

Control ID	Control Description	AWS Config Rule	Guidance
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
AC.3.014	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
AC.3.014	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
AC.3.014	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
AC.3.014	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
AC.3.014	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
AC.3.014	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
AU.3.046	Alert in the event of an audit logging process failure.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
AU.3.046	Alert in the event of an audit logging process failure.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
AU.3.046	Alert in the event of an audit logging process failure.	<a href="#">cloud-trail-cloudwatch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	<a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a>	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.

Control ID	Control Description	AWS Config Rule	Guidance
AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.
AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.
AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
AU.3.051	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
CM.3.068	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
CM.3.068	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
CM.3.068	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	Control Description	AWS Config Rule	Guidance
CM.3.068	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
IA.3.083	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
IA.3.083	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
IA.3.085	Prevent the reuse of identifiers for a defined period.	<a href="#">iam-password-policy</a> (p. 154)	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
IA.3.086	Disable identifiers after a defined period of inactivity.	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
IA.3.086	Disable identifiers after a defined period of inactivity.	<a href="#">iam-password-policy</a> (p. 154)	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
RE.3.139	Regularly perform complete, comprehensive, and resilient data backups as organizationally defined.	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.
RE.3.139	Regularly perform complete, comprehensive, and resilient data backups as organizationally defined.	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.
RE.3.139	Regularly perform complete, comprehensive, and resilient data backups as organizationally defined.	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.

Control ID	Control Description	AWS Config Rule	Guidance
RE.3.139	Regularly perform complete, comprehensive, and resilient data backups as organizationally defined.	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
CA.3.161	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">account-part-of-organizations (p. 108)</a>	Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">cloudtrail-security-trail-enabled (p. 118)</a>	This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">ebs-optimized-instance (p. 131)</a>	An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a>	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">rds-instance-deletion-protection-enabled (p. 166)</a>	Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
SC.3.182	Prevent unauthorized and unintended information transfer via shared system resources.	<a href="#">ec2-volume-in-use-check (p. 137)</a>	This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.185	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.3.185	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.3.185	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.3.185	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.185	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.3.185	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.3.187	Establish and manage cryptographic keys for cryptography employed in organizational systems.	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.
SC.3.187	Establish and manage cryptographic keys for cryptography employed in organizational systems.	<a href="#">cmk-backing-key-rotation-enabled (p. 123)</a>	Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.190	Protect the authenticity of communications sessions.	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.3.190	Protect the authenticity of communications sessions.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.3.190	Protect the authenticity of communications sessions.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">ec2-efs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.

## Template

The template is available on GitHub: [Operational Best Practices for CMMC Level 3](#).

## Operational Best Practices for CMMC Level 4

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Cybersecurity Maturity Model Certification (CMMC) Level 4 and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more CMMC Level 4 controls. A CMMC Level 4 control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This Conformance Pack was validated by AWS Security Assurance Services LLC (AWS SAS), which is a team of Payment Card Industry Qualified Security Assessors (QSAs), HITRUST Certified Common Security Framework Practitioners (CCSFPs), and compliance professionals certified to provide guidance and assessments for various industry frameworks. AWS SAS professionals designed this Conformance Pack to enable a customer to align to a subset of the CMMC Level 4.

**AWS Region:** Due to tentative guidance provided by the DoD and the CMMC Accreditation Body with respect to FedRAMP reciprocity for CMMC Level 3 - 5, it is recommended that customers use AWS GovCloud (US) regions at this time for any workloads that require compliance with CMMC Level 3 - 5. As such, conformance pack templates for CMMC Levels 3 - 5 are not available within the conformance pack console to avoid confusion. Customers may independently install Config rules that map the tentative guidance for CMMC Level 3-5 (without a conformance pack template) via CloudFormation using the sample YAML file linked within this document.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-password-policy (p. 154)</a>	The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational

Control ID	Control Description	AWS Config Rule	Guidance
			Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">ec2-imdsv2-check (p. 132)</a>	Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-password-policy</a> (p. 154)	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
IA.1.076	Identify information system users, processes acting on behalf of users, or devices.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	Control Description	AWS Config Rule	Guidance
IA.1.076	Identify information system users, processes acting on behalf of users, or devices.	<a href="#">emr-kerberos-enabled (p. 145)</a>	<p>The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.</p>

Control ID	Control Description	AWS Config Rule	Guidance
IA.1.076	Identify information system users, processes acting on behalf of users, or devices.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
IA.1.076	Identify information system users, processes acting on behalf of users, or devices.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
IA.1.076	Identify information system users, processes acting on behalf of users, or devices.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
IA.1.076	Identify information system users, processes acting on behalf of users, or devices.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
IA.1.077	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
IA.1.077	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
IA.1.077	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.

Control ID	Control Description	AWS Config Rule	Guidance
IA.1.077	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), and <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">alb-http-to-https-redirection-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.176	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
SI.1.210	Identify, report, and correct information and information system flaws in a timely manner.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
SI.1.210	Identify, report, and correct information and information system flaws in a timely manner.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
SI.1.211	Provide protection from malicious code at appropriate locations within organizational information systems.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">emr-kerberos-enabled (p. 145)</a>	<p>The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.</p>
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">iam-group-has-users-check (p. 153)</a>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">ec2-imdsv2-check (p. 132)</a>	Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.008	Use non-privileged accounts or roles when accessing nonsecurity functions.	<a href="#">emr-kerberos-enabled (p. 145)</a>	<p>The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.</p>
AC.2.008	Use non-privileged accounts or roles when accessing nonsecurity functions.	<a href="#">iam-group-has-users-check (p. 153)</a>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.008	Use non-privileged accounts or roles when accessing nonsecurity functions.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC.2.008	Use non-privileged accounts or roles when accessing nonsecurity functions.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
AC.2.008	Use non-privileged accounts or roles when accessing nonsecurity functions.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.008	Use non-privileged accounts or roles when accessing nonsecurity functions.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
AC.2.008	Use non-privileged accounts or roles when accessing nonsecurity functions.	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.013	Monitor and control remote access sessions.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
AC.2.013	Monitor and control remote access sessions.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
AC.2.013	Monitor and control remote access sessions.	<a href="#">cloud-trail-cloudwatch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
AU.2.041	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
AU.2.041	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
AU.2.041	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
AU.2.041	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
AU.2.041	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
AU.2.041	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
AU.2.041	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">cw-loggroup-retention-period-check (p. 125)</a>	Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events.
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	<a href="#">ec2-security-group-attached-to-eni (p. 137)</a>	This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	<a href="#">ec2-stopped-instance (p. 137)</a>	Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards.
CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	<a href="#">ec2-volume-in-use-check (p. 137)</a>	This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality.
CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	<a href="#">eip-attached (p. 139)</a>	This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">ec2-volume-inuse-check (p. 137)</a>	This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality.
CM.2.063	Control and monitor user-installed software.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.063	Control and monitor user-installed software.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
CM.2.064	Establish and enforce security configuration settings for information technology products employed in organizational systems.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.064	Establish and enforce security configuration settings for information technology products employed in organizational systems.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
CM.2.064	Establish and enforce security configuration settings for information technology products employed in organizational systems.	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
CM.2.064	Establish and enforce security configuration settings for information technology products employed in organizational systems.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.064	Establish and enforce security configuration settings for information technology products employed in organizational systems.	<a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a>	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.
CM.2.064	Establish and enforce security configuration settings for information technology products employed in organizational systems.	<a href="#">account-part-of-organizations (p. 108)</a>	Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data.
CM.2.064	Establish and enforce security configuration settings for information technology products employed in organizational systems.	<a href="#">cloudtrail-security-trail-enabled (p. 118)</a>	This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.065	Track, review, approve, or disapprove, and log changes to organizational systems.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
CM.2.065	Track, review, approve, or disapprove, and log changes to organizational systems.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.065	Track, review, approve, or disapprove, and log changes to organizational systems.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
CM.2.065	Track, review, approve, or disapprove, and log changes to organizational systems.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.065	Track, review, approve, or disapprove, and log changes to organizational systems.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
CM.2.065	Track, review, approve, or disapprove, and log changes to organizational systems.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.065	Track, review, approve, or disapprove, and log changes to organizational systems.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
IA.2.078	Enforce a minimum password complexity and change of characters when new passwords are created.	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
IA.2.079	Prohibit password reuse for a specified number of generations.	<a href="#">iam-password-policy</a> (p. 154)	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.

Control ID	Control Description	AWS Config Rule	Guidance
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">ec2-ebs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
IR.2.092	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), and <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
IR.2.092	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	<a href="#">lambda-dlq-check (p. 161)</a>	Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed.

Control ID	Control Description	AWS Config Rule	Guidance
IR.2.092	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
IR.2.093	Detect and report events.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.

Control ID	Control Description	AWS Config Rule	Guidance
IR.2.093	Detect and report events.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
IR.2.093	Detect and report events.	<a href="#">lambda-dlq-check (p. 161)</a>	Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed.
MA.2.113	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.

Control ID	Control Description	AWS Config Rule	Guidance
MA.2.113	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
RE.2.137	Regularly perform and test data backups.	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.
RE.2.137	Regularly perform and test data backups.	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.

Control ID	Control Description	AWS Config Rule	Guidance
RE.2.137	Regularly perform and test data backups.	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
RE.2.137	Regularly perform and test data backups.	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
RE.2.137	Regularly perform and test data backups.	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.

Control ID	Control Description	AWS Config Rule	Guidance
RM.2.142	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
SI.2.214	Monitor system security alerts and advisories and take action in response.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.

Control ID	Control Description	AWS Config Rule	Guidance
SI.2.214	Monitor system security alerts and advisories and take action in response.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
SI.2.214	Monitor system security alerts and advisories and take action in response.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
SI.2.214	Monitor system security alerts and advisories and take action in response.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
SI.2.216	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
SI.2.216	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.

Control ID	Control Description	AWS Config Rule	Guidance
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.

Control ID	Control Description	AWS Config Rule	Guidance
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.

Control ID	Control Description	AWS Config Rule	Guidance
AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.

Control ID	Control Description	AWS Config Rule	Guidance
AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.

Control ID	Control Description	AWS Config Rule	Guidance
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	Control Description	AWS Config Rule	Guidance
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.

Control ID	Control Description	AWS Config Rule	Guidance
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.

Control ID	Control Description	AWS Config Rule	Guidance
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.

Control ID	Control Description	AWS Config Rule	Guidance
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
AC.3.014	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
AC.3.014	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
AC.3.014	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
AC.3.014	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
AC.3.014	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
AC.3.014	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
AU.3.046	Alert in the event of an audit logging process failure.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
AU.3.046	Alert in the event of an audit logging process failure.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
AU.3.046	Alert in the event of an audit logging process failure.	<a href="#">cloud-trail-cloudwatch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	<a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a>	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.

Control ID	Control Description	AWS Config Rule	Guidance
AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.
AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.
AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
AU.3.051	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
CM.3.068	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
CM.3.068	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
CM.3.068	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	Control Description	AWS Config Rule	Guidance
CM.3.068	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
IA.3.083	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
IA.3.083	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
IA.3.085	Prevent the reuse of identifiers for a defined period.	<a href="#">iam-password-policy</a> (p. 154)	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
IA.3.086	Disable identifiers after a defined period of inactivity.	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
IA.3.086	Disable identifiers after a defined period of inactivity.	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
RE.3.139	Regularly perform complete, comprehensive, and resilient data backups as organizationally defined.	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.
RE.3.139	Regularly perform complete, comprehensive, and resilient data backups as organizationally defined.	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.
RE.3.139	Regularly perform complete, comprehensive, and resilient data backups as organizationally defined.	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.

Control ID	Control Description	AWS Config Rule	Guidance
RE.3.139	Regularly perform complete, comprehensive, and resilient data backups as organizationally defined.	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
CA.3.161	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">account-part-of-organizations (p. 108)</a>	Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">cloudtrail-security-trail-enabled (p. 118)</a>	This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">ebs-optimized-instance (p. 131)</a>	An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a>	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">rds-instance-deletion-protection-enabled (p. 166)</a>	Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
SC.3.182	Prevent unauthorized and unintended information transfer via shared system resources.	<a href="#">ec2-volume-in-use-check (p. 137)</a>	This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.185	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.3.185	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.3.185	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.3.185	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.185	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.3.185	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.3.187	Establish and manage cryptographic keys for cryptography employed in organizational systems.	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.
SC.3.187	Establish and manage cryptographic keys for cryptography employed in organizational systems.	<a href="#">cmk-backing-key-rotation-enabled (p. 123)</a>	Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.190	Protect the authenticity of communications sessions.	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.3.190	Protect the authenticity of communications sessions.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.3.190	Protect the authenticity of communications sessions.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">ec2-ebs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.

Control ID	Control Description	AWS Config Rule	Guidance
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.

Control ID	Control Description	AWS Config Rule	Guidance
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	Control Description	AWS Config Rule	Guidance
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
AM.4.226	Employ a capability to discover and identify systems with specific component attributes (e.g., firmware level, OS type) within your inventory.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
AM.4.226	Employ a capability to discover and identify systems with specific component attributes (e.g., firmware level, OS type) within your inventory.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
AM.4.226	Employ a capability to discover and identify systems with specific component attributes (e.g., firmware level, OS type) within your inventory.	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
AU.4.053	Automate analysis of audit logs to identify and act on critical indicators (TTPs) and/or organizationally defined suspicious activity.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
AU.4.053	Automate analysis of audit logs to identify and act on critical indicators (TTPs) and/or organizationally defined suspicious activity.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), and <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
AU.4.053	Automate analysis of audit logs to identify and act on critical indicators (TTPs) and/or organizationally defined suspicious activity.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
AU.4.053	Automate analysis of audit logs to identify and act on critical indicators (TTPs) and/or organizationally defined suspicious activity.	<a href="#">ec2-instance-detailed-monitoring-enabled (p. 132)</a>	Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance.

Control ID	Control Description	AWS Config Rule	Guidance
AU.4.054	Review audit information for broad activity in addition to per-machine activity.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
RM.4.151	Perform scans for unauthorized ports available across perimeter network boundaries over the organization's Internet network boundaries and other organizationally defined boundaries.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
RM.4.151	Perform scans for unauthorized ports available across perimeter network boundaries over the organization's Internet network boundaries and other organizationally defined boundaries.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
RM.4.151	Perform scans for unauthorized ports available across perimeter network boundaries over the organization's Internet network boundaries and other organizationally defined boundaries.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	Control Description	AWS Config Rule	Guidance
RM.4.151	Perform scans for unauthorized ports available across perimeter network boundaries over the organization's Internet network boundaries and other organizationally defined boundaries.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.

## Template

The template is available on GitHub: [Operational Best Practices for CMMC Level 4](#).

## Operational Best Practices for CMMC Level 5

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Cybersecurity Maturity Model Certification (CMMC) Level 5 and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more CMMC Level 5 controls. A CMMC Level 5 control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This Conformance Pack was validated by AWS Security Assurance Services LLC (AWS SAS), which is a team of Payment Card Industry Qualified Security Assessors (QSAs), HITRUST Certified Common Security Framework Practitioners (CCSFPs), and compliance professionals certified to provide guidance and assessments for various industry frameworks. AWS SAS professionals designed this Conformance Pack to enable a customer to align to a subset of the CMMC Level 5.

**AWS Region:** Due to tentative guidance provided by the DoD and the CMMC Accreditation Body with respect to FedRAMP reciprocity for CMMC Level 3 - 5, it is recommended that customers use AWS GovCloud (US) regions at this time for any workloads that require compliance with CMMC Level 3 - 5. As such, conformance pack templates for CMMC Levels 3 - 5 are not available within the conformance pack console to avoid confusion. Customers may independently install Config rules that map the tentative guidance for CMMC Level 3-5 (without a conformance pack template) via CloudFormation using the sample YAML file linked within this document.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-password-policy (p. 154)</a>	The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational

Control ID	Control Description	AWS Config Rule	Guidance
			Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">ec2-imdsv2-check (p. 132)</a>	Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata.
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-password-policy</a> (p. 154)	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
AC.1.003	Verify and control/limit connections to and use of external information systems.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
IA.1.076	Identify information system users, processes acting on behalf of users, or devices.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	Control Description	AWS Config Rule	Guidance
IA.1.076	Identify information system users, processes acting on behalf of users, or devices.	<a href="#">emr-kerberos-enabled (p. 145)</a>	<p>The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.</p>

Control ID	Control Description	AWS Config Rule	Guidance
IA.1.076	Identify information system users, processes acting on behalf of users, or devices.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
IA.1.076	Identify information system users, processes acting on behalf of users, or devices.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
IA.1.076	Identify information system users, processes acting on behalf of users, or devices.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
IA.1.076	Identify information system users, processes acting on behalf of users, or devices.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
IA.1.077	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
IA.1.077	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
IA.1.077	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.

Control ID	Control Description	AWS Config Rule	Guidance
IA.1.077	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), and <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">alb-http-to-https-redirection-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
SC.1.176	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
SI.1.210	Identify, report, and correct information and information system flaws in a timely manner.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
SI.1.210	Identify, report, and correct information and information system flaws in a timely manner.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
SI.1.211	Provide protection from malicious code at appropriate locations within organizational information systems.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">emr-kerberos-enabled (p. 145)</a>	<p>The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.</p>
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">iam-group-has-users-check (p. 153)</a>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">ec2-imdsv2-check (p. 132)</a>	Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.008	Use non-privileged accounts or roles when accessing nonsecurity functions.	<a href="#">emr-kerberos-enabled (p. 145)</a>	<p>The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.</p>
AC.2.008	Use non-privileged accounts or roles when accessing nonsecurity functions.	<a href="#">iam-group-has-users-check (p. 153)</a>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.008	Use non-privileged accounts or roles when accessing nonsecurity functions.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC.2.008	Use non-privileged accounts or roles when accessing nonsecurity functions.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
AC.2.008	Use non-privileged accounts or roles when accessing nonsecurity functions.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.008	Use non-privileged accounts or roles when accessing nonsecurity functions.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
AC.2.008	Use non-privileged accounts or roles when accessing nonsecurity functions.	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.013	Monitor and control remote access sessions.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
AC.2.013	Monitor and control remote access sessions.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
AC.2.013	Monitor and control remote access sessions.	<a href="#">cloud-trail-cloudwatch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
AU.2.041	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
AU.2.041	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
AU.2.041	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
AU.2.041	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
AU.2.041	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
AU.2.041	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
AU.2.041	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">cw-loggroup-retention-period-check (p. 125)</a>	Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events.
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	<a href="#">ec2-security-group-attached-to-eni (p. 137)</a>	This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	<a href="#">ec2-stopped-instance (p. 137)</a>	Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards.
CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	<a href="#">ec2-volume-in-use-check (p. 137)</a>	This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality.
CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	<a href="#">eip-attached (p. 139)</a>	This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">ec2-volume-inuse-check (p. 137)</a>	This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality.
CM.2.063	Control and monitor user-installed software.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.063	Control and monitor user-installed software.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
CM.2.064	Establish and enforce security configuration settings for information technology products employed in organizational systems.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.064	Establish and enforce security configuration settings for information technology products employed in organizational systems.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
CM.2.064	Establish and enforce security configuration settings for information technology products employed in organizational systems.	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
CM.2.064	Establish and enforce security configuration settings for information technology products employed in organizational systems.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.064	Establish and enforce security configuration settings for information technology products employed in organizational systems.	<a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a>	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.
CM.2.064	Establish and enforce security configuration settings for information technology products employed in organizational systems.	<a href="#">account-part-of-organizations (p. 108)</a>	Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data.
CM.2.064	Establish and enforce security configuration settings for information technology products employed in organizational systems.	<a href="#">cloudtrail-security-trail-enabled (p. 118)</a>	This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.065	Track, review, approve, or disapprove, and log changes to organizational systems.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
CM.2.065	Track, review, approve, or disapprove, and log changes to organizational systems.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.065	Track, review, approve, or disapprove, and log changes to organizational systems.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
CM.2.065	Track, review, approve, or disapprove, and log changes to organizational systems.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.065	Track, review, approve, or disapprove, and log changes to organizational systems.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
CM.2.065	Track, review, approve, or disapprove, and log changes to organizational systems.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
CM.2.065	Track, review, approve, or disapprove, and log changes to organizational systems.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
IA.2.078	Enforce a minimum password complexity and change of characters when new passwords are created.	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
IA.2.079	Prohibit password reuse for a specified number of generations.	<a href="#">iam-password-policy</a> (p. 154)	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">alb-http-to-https-redirection-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.

Control ID	Control Description	AWS Config Rule	Guidance
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">ec2-ebs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
IA.2.081	Store and transmit only cryptographically-protected passwords.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
IR.2.092	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), and <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
IR.2.092	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	<a href="#">lambda-dlq-check (p. 161)</a>	Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed.

Control ID	Control Description	AWS Config Rule	Guidance
IR.2.092	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
IR.2.093	Detect and report events.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.

Control ID	Control Description	AWS Config Rule	Guidance
IR.2.093	Detect and report events.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
IR.2.093	Detect and report events.	<a href="#">lambda-dlq-check (p. 161)</a>	Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed.
MA.2.113	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.

Control ID	Control Description	AWS Config Rule	Guidance
MA.2.113	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
RE.2.137	Regularly perform and test data backups.	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.
RE.2.137	Regularly perform and test data backups.	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.

Control ID	Control Description	AWS Config Rule	Guidance
RE.2.137	Regularly perform and test data backups.	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
RE.2.137	Regularly perform and test data backups.	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
RE.2.137	Regularly perform and test data backups.	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.

Control ID	Control Description	AWS Config Rule	Guidance
RM.2.142	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
SI.2.214	Monitor system security alerts and advisories and take action in response.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.

Control ID	Control Description	AWS Config Rule	Guidance
SI.2.214	Monitor system security alerts and advisories and take action in response.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
SI.2.214	Monitor system security alerts and advisories and take action in response.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
SI.2.214	Monitor system security alerts and advisories and take action in response.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
SI.2.216	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
SI.2.216	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.

Control ID	Control Description	AWS Config Rule	Guidance
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	<p>To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.</p>
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">elb-logging-enabled (p. 144)</a>	<p>Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.

Control ID	Control Description	AWS Config Rule	Guidance
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
SI.2.217	Identify unauthorized use of organizational systems.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.

Control ID	Control Description	AWS Config Rule	Guidance
AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.

Control ID	Control Description	AWS Config Rule	Guidance
AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.

Control ID	Control Description	AWS Config Rule	Guidance
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	Control Description	AWS Config Rule	Guidance
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.

Control ID	Control Description	AWS Config Rule	Guidance
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.

Control ID	Control Description	AWS Config Rule	Guidance
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.

Control ID	Control Description	AWS Config Rule	Guidance
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
AC.3.014	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
AC.3.014	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
AC.3.014	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
AC.3.014	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
AC.3.014	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
AC.3.014	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
AU.3.046	Alert in the event of an audit logging process failure.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
AU.3.046	Alert in the event of an audit logging process failure.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
AU.3.046	Alert in the event of an audit logging process failure.	<a href="#">cloud-trail-cloudwatch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	<a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a>	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.

Control ID	Control Description	AWS Config Rule	Guidance
AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.
AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.
AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
AU.3.051	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
CM.3.068	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
CM.3.068	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
CM.3.068	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	Control Description	AWS Config Rule	Guidance
CM.3.068	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
IA.3.083	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
IA.3.083	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
IA.3.085	Prevent the reuse of identifiers for a defined period.	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
IA.3.086	Disable identifiers after a defined period of inactivity.	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
IA.3.086	Disable identifiers after a defined period of inactivity.	<a href="#">iam-password-policy</a> (p. 154)	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
RE.3.139	Regularly perform complete, comprehensive, and resilient data backups as organizationally defined.	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.
RE.3.139	Regularly perform complete, comprehensive, and resilient data backups as organizationally defined.	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.
RE.3.139	Regularly perform complete, comprehensive, and resilient data backups as organizationally defined.	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.

Control ID	Control Description	AWS Config Rule	Guidance
RE.3.139	Regularly perform complete, comprehensive, and resilient data backups as organizationally defined.	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
CA.3.161	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">account-part-of-organizations (p. 108)</a>	Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">cloudtrail-security-trail-enabled (p. 118)</a>	This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">ebs-optimized-instance (p. 131)</a>	An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a>	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">rds-instance-deletion-protection-enabled (p. 166)</a>	Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
SC.3.182	Prevent unauthorized and unintended information transfer via shared system resources.	<a href="#">ec2-volume-in-use-check (p. 137)</a>	This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.185	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.3.185	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.3.185	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.3.185	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.185	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.3.185	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.3.187	Establish and manage cryptographic keys for cryptography employed in organizational systems.	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.
SC.3.187	Establish and manage cryptographic keys for cryptography employed in organizational systems.	<a href="#">cmk-backing-key-rotation-enabled (p. 123)</a>	Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.190	Protect the authenticity of communications sessions.	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.3.190	Protect the authenticity of communications sessions.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.3.190	Protect the authenticity of communications sessions.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">ec2-ebs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
SC.3.191	Protect the confidentiality of CUI at rest.	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.

Control ID	Control Description	AWS Config Rule	Guidance
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.

Control ID	Control Description	AWS Config Rule	Guidance
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	Control Description	AWS Config Rule	Guidance
AC.4.023	Control information flows between security domains on connected systems.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
AM.4.226	Employ a capability to discover and identify systems with specific component attributes (e.g., firmware level, OS type) within your inventory.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
AM.4.226	Employ a capability to discover and identify systems with specific component attributes (e.g., firmware level, OS type) within your inventory.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
AM.4.226	Employ a capability to discover and identify systems with specific component attributes (e.g., firmware level, OS type) within your inventory.	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
AU.4.053	Automate analysis of audit logs to identify and act on critical indicators (TTPs) and/or organizationally defined suspicious activity.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
AU.4.053	Automate analysis of audit logs to identify and act on critical indicators (TTPs) and/or organizationally defined suspicious activity.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), and <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
AU.4.053	Automate analysis of audit logs to identify and act on critical indicators (TTPs) and/or organizationally defined suspicious activity.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
AU.4.053	Automate analysis of audit logs to identify and act on critical indicators (TTPs) and/or organizationally defined suspicious activity.	<a href="#">ec2-instance-detailed-monitoring-enabled (p. 132)</a>	Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance.

Control ID	Control Description	AWS Config Rule	Guidance
AU.4.054	Review audit information for broad activity in addition to per-machine activity.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
RM.4.151	Perform scans for unauthorized ports available across perimeter network boundaries over the organization's Internet network boundaries and other organizationally defined boundaries.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
RM.4.151	Perform scans for unauthorized ports available across perimeter network boundaries over the organization's Internet network boundaries and other organizationally defined boundaries.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
RM.4.151	Perform scans for unauthorized ports available across perimeter network boundaries over the organization's Internet network boundaries and other organizationally defined boundaries.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	Control Description	AWS Config Rule	Guidance
RM.4.151	Perform scans for unauthorized ports available across perimeter network boundaries over the organization's Internet network boundaries and other organizationally defined boundaries.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
AU.5.055	Identify assets not reporting audit logs and assure appropriate organizationally defined systems are logging.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
AU.5.055	Identify assets not reporting audit logs and assure appropriate organizationally defined systems are logging.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
AU.5.055	Identify assets not reporting audit logs and assure appropriate organizationally defined systems are logging.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	Control Description	AWS Config Rule	Guidance
AU.5.055	Identify assets not reporting audit logs and assure appropriate organizationally defined systems are logging.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
AU.5.055	Identify assets not reporting audit logs and assure appropriate organizationally defined systems are logging.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
AU.5.055	Identify assets not reporting audit logs and assure appropriate organizationally defined systems are logging.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
AU.5.055	Identify assets not reporting audit logs and assure appropriate organizationally defined systems are logging.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
AU.5.055	Identify assets not reporting audit logs and assure appropriate organizationally defined systems are logging.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
AU.5.055	Identify assets not reporting audit logs and assure appropriate organizationally defined systems are logging.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
AU.5.055	Identify assets not reporting audit logs and assure appropriate organizationally defined systems are logging.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AU.5.055	Identify assets not reporting audit logs and assure appropriate organizationally defined systems are logging.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
CM.5.074	Verify the integrity and correctness of security critical or essential software as defined by the organization (e.g., roots of trust, formal verification, or cryptographic signatures).	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
CM.5.074	Verify the integrity and correctness of security critical or essential software as defined by the organization (e.g., roots of trust, formal verification, or cryptographic signatures).	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
CM.5.074	Verify the integrity and correctness of security critical or essential software as defined by the organization (e.g., roots of trust, formal verification, or cryptographic signatures).	<a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a>	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.
CM.5.074	Verify the integrity and correctness of security critical or essential software as defined by the organization (e.g., roots of trust, formal verification, or cryptographic signatures).	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
IR.5.102	Use a combination of manual and automated, real-time responses to anomalous activities that match incident patterns.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
IR.5.102	Use a combination of manual and automated, real-time responses to anomalous activities that match incident patterns.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
RE.5.140	Ensure information processing facilities meet organizationally defined information security continuity, redundancy, and availability requirements.	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.
RE.5.140	Ensure information processing facilities meet organizationally defined information security continuity, redundancy, and availability requirements.	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.
RE.5.140	Ensure information processing facilities meet organizationally defined information security continuity, redundancy, and availability requirements.	<a href="#">ebs-optimized-instance (p. 131)</a>	An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance.

Control ID	Control Description	AWS Config Rule	Guidance
RE.5.140	Ensure information processing facilities meet organizationally defined information security continuity, redundancy, and availability requirements.	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
RE.5.140	Ensure information processing facilities meet organizationally defined information security continuity, redundancy, and availability requirements.	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.

Control ID	Control Description	AWS Config Rule	Guidance
RE.5.140	Ensure information processing facilities meet organizationally defined information security continuity, redundancy, and availability requirements.	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
RE.5.140	Ensure information processing facilities meet organizationally defined information security continuity, redundancy, and availability requirements.	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.

Control ID	Control Description	AWS Config Rule	Guidance
RE.5.140	Ensure information processing facilities meet organizationally defined information security continuity, redundancy, and availability requirements.	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.
RE.5.140	Ensure information processing facilities meet organizationally defined information security continuity, redundancy, and availability requirements.	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.

Control ID	Control Description	AWS Config Rule	Guidance
RE.5.140	Ensure information processing facilities meet organizationally defined information security continuity, redundancy, and availability requirements.	<a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a>	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.
RE.5.140	Ensure information processing facilities meet organizationally defined information security continuity, redundancy, and availability requirements.	<a href="#">rds-instance-deletion-protection-enabled (p. 166)</a>	Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
SC.5.230	Enforce port and protocol compliance.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
SC.5.230	Enforce port and protocol compliance.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
SC.5.230	Enforce port and protocol compliance.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	Control Description	AWS Config Rule	Guidance
SC.5.230	Enforce port and protocol compliance.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
SC.5.208	Employ organizationally defined and tailored boundary protections in addition to commercially available solutions.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
SC.5.208	Employ organizationally defined and tailored boundary protections in addition to commercially available solutions.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
SC.5.208	Employ organizationally defined and tailored boundary protections in addition to commercially available solutions.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	Control Description	AWS Config Rule	Guidance
SC.5.208	Employ organizationally defined and tailored boundary protections in addition to commercially available solutions.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
SI.5.223	Monitor individuals and system components on an ongoing basis for anomalous or suspicious behavior.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
SI.5.223	Monitor individuals and system components on an ongoing basis for anomalous or suspicious behavior.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), and <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
SI.5.223	Monitor individuals and system components on an ongoing basis for anomalous or suspicious behavior.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
SI.5.223	Monitor individuals and system components on an ongoing basis for anomalous or suspicious behavior.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.

Control ID	Control Description	AWS Config Rule	Guidance
SI.5.223	Monitor individuals and system components on an ongoing basis for anomalous or suspicious behavior.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
SI.5.223	Monitor individuals and system components on an ongoing basis for anomalous or suspicious behavior.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
SI.5.223	Monitor individuals and system components on an ongoing basis for anomalous or suspicious behavior.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
SI.5.223	Monitor individuals and system components on an ongoing basis for anomalous or suspicious behavior.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
SI.5.223	Monitor individuals and system components on an ongoing basis for anomalous or suspicious behavior.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
SI.5.223	Monitor individuals and system components on an ongoing basis for anomalous or suspicious behavior.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
SI.5.223	Monitor individuals and system components on an ongoing basis for anomalous or suspicious behavior.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.

## Template

The template is available on GitHub: [Operational Best Practices for CMMC Level 5](#).

## Operational Best Practices for Compute Services

This pack contains AWS Config rules based on Compute Services. For more information, see [Compute for any workload](#). This Conformance Pack has been designed for compatibility with the majority of AWS regions and to not require setting of any Parameters. Additional managed rules that require parameters to be set for your environment and/or for your specific region can be found at: [List of AWS Config Managed Rules](#).

See Parameters section for names and descriptions of required parameters.

The template is available on GitHub: [Operational Best Practices for Compute Services](#).

## Operational Best Practices for Data Resiliency

This Conformance Pack has been designed for compatibility with the majority of AWS regions and to not require setting of any Parameters. Additional managed rules that require parameters to be set for your environment and/or for your specific region can be found at: [List of AWS Config Managed Rules](#).

See Parameters section for names and descriptions of required parameters.

The template is available on GitHub: [Operational Best Practices for Data Resiliency](#).

## Operational Best Practices for Databases Services

This pack contains AWS Config rules based on Databases Services. For more information, see [Databases on AWS](#). This Conformance Pack has been designed for compatibility with the majority of AWS regions and to not require setting of any Parameters. Additional managed rules that require parameters to be set for your environment and/or for your specific region can be found at: [List of AWS Config Managed Rules](#).

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

See Parameters section for names and descriptions of required parameters.

The template is available on GitHub: [Operational Best Practices for Databases Services](#).

## Operational Best Practices for Data Lakes and Analytics Services

This pack contains AWS Config rules for Data Lakes and Analytics Services. For more information, see [Data Lakes and Analytics on AWS](#). This Conformance Pack has been designed for compatibility with the majority of AWS regions and to not require setting of any Parameters. Additional managed rules that require parameters to be set for your environment and/or for your specific region can be found at: [List of AWS Config Managed Rules](#).

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

See Parameters section for names and descriptions of required parameters.

The template is available on GitHub: [Operational Best Practices for Data Lakes and Analytics Services](#).

## Operational Best Practices for EC2

This pack contains AWS Config rules based on EC2. This Conformance Pack has been designed for compatibility with the majority of AWS regions and to not require setting of any Parameters. Additional managed rules that require parameters to be set for your environment and/or for your specific region can be found at: [List of AWS Config Managed Rules](#).

See Parameters section for names and descriptions of required parameters.

The template is available on GitHub: [Operational Best Practices for EC2](#).

## Operational Best Practices for Encryption and Key Management

This Conformance Pack has been designed for compatibility with the majority of AWS regions and to not require setting of any Parameters. Additional managed rules that require parameters to be set for your environment and/or for your specific region can be found at: [List of AWS Config Managed Rules](#).

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

See Parameters section for names and descriptions of required parameters.

The template is available on GitHub: [Operational Best Practices for Encryption and Key Management](#).

## Operational Best Practices for Esquema Nacional de Seguridad (ENS) Low

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between Spain Esquema Nacional de Seguridad (ENS) Low framework controls and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more Spain ENS Low controls. A Spain ENS control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This sample conformance pack template contains mappings to controls within the Spain ENS Low framework, as last updated on 2020/10/23.

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

Control ID	AWS Config Rule	Guidance
Article_16	<a href="#">access-keys-rotated (p. 107)</a>	The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.
Article_16	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
Article_16	<a href="#">iam-password-policy (p. 154)</a>	The identities and the credentials are issued, managed, and verified based on an organizational IAM password

Control ID	AWS Config Rule	Guidance
		<p>policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>
Article_16	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.</p>

Control ID	AWS Config Rule	Guidance
Article_16	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
Article_16	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
Article_16	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
Article_16	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies.

AWS Config Developer Guide  
Operational Best Practices for Esquema  
Nacional de Seguridad (ENS) Low

Control ID	AWS Config Rule	Guidance
Article_16	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling s3_bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
Article_16	<a href="#">secretsmanager-rotation-enabled-check (p. 183)</a>	This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised.
Article_20	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
Article_20	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	AWS Config Rule	Guidance
Article_20	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
Article_21	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
Article_21	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
Article_21	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
Article_21	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
Article_21	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
Article_21	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.

Control ID	AWS Config Rule	Guidance
Article_21	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.
Article_21	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.
Article_21	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.
Article_21	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
Article_21	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
Article_21	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.
Article_21	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.
Article_21	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
Article_21	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
Article_21	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
Article_21	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	AWS Config Rule	Guidance
Article_22	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
Article_22	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
Article_22	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.

AWS Config Developer Guide  
Operational Best Practices for Esquema  
Nacional de Seguridad (ENS) Low

Control ID	AWS Config Rule	Guidance
Article_22	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
Article_22	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
Article_22	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

AWS Config Developer Guide  
Operational Best Practices for Esquema  
Nacional de Seguridad (ENS) Low

Control ID	AWS Config Rule	Guidance
Article_22	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
Article_22	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
Article_23	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
Article_23	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	AWS Config Rule	Guidance
Article_23	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
Article_23	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
Article_23	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
Article_23	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.

Control ID	AWS Config Rule	Guidance
Article_23	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.
Article_23	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
Article_23	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.

AWS Config Developer Guide  
Operational Best Practices for Esquema  
Nacional de Seguridad (ENS) Low

Control ID	AWS Config Rule	Guidance
Article_24	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
Article_24	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
Article_24	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
Article_24	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	AWS Config Rule	Guidance
Article_24	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.
Article_24	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
Article_24	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	AWS Config Rule	Guidance
Article_24	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
Article_24	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment.
Article_24	<a href="#">codebuild-project-source-repo-url-check (p. 123)</a>	Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, user name and password within AWS Codebuild project environments. Use OAuth instead of personal access tokens or a user name and password to grant authorization for accessing GitHub or Bitbucket repositories.
Article_24	<a href="#">lambda-dlq-check (p. 161)</a>	Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed.

Control ID	AWS Config Rule	Guidance
Article_25	<a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a>	The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.
Article_25	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.
Article_25	<a href="#">dynamodb-autoscaling-enabled (p. 128)</a>	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.

Control ID	AWS Config Rule	Guidance
Article_25	<a href="#">dynamodb-throughput-limit-check (p. 130)</a>	Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set <code>accountRCUThresholdPercentage</code> (Config Default: 80) and <code>accountWCUThresholdPercentage</code> (Config Default: 80) parameters. The actual values should reflect your organization's policies.
Article_25	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
Article_25	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.

Control ID	AWS Config Rule	Guidance
Article_25	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
Article_25	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
Article_25	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.

Control ID	AWS Config Rule	Guidance
Article_25	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.
Article_25	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.
Article_31	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
Article_31	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
Article_31	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	AWS Config Rule	Guidance
Article_31	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
Article_31	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
Article_31	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

AWS Config Developer Guide  
Operational Best Practices for Esquema  
Nacional de Seguridad (ENS) Low

Control ID	AWS Config Rule	Guidance
Article_31	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
Article_33	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
Article_33	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.
Article_35	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	AWS Config Rule	Guidance
Article_35	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
Article_37	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
Article_37	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
Article_37	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
Article_37	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.

Control ID	AWS Config Rule	Guidance
Article_37	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
Article_37	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
Article_37	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
Article_37	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
Article_37	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
Article_37	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
Article_37	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.

Control ID	AWS Config Rule	Guidance
Article_37	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
Article_37	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
Article_37	<a href="#">codebuild-project-source-repo-url-check (p. 123)</a>	Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, user name and password within AWS Codebuild project environments. Use OAuth instead of personal access tokens or a user name and password to grant authorization for accessing GitHub or Bitbucket repositories.
Article_37	<a href="#">lambda-dlq-check (p. 161)</a>	Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed.

AWS Config Developer Guide  
Operational Best Practices for Esquema  
Nacional de Seguridad (ENS) Low

---

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.1	<a href="#">access-keys-rotated (p. 107)</a>	<p>The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.</p>
Appendix_II_4.2.1	<a href="#">iam-group-has-users-check (p. 153)</a>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.</p>

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.1	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>
Appendix_II_4.2.1	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.</p>

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.1	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
Appendix_II_4.2.1	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
Appendix_II_4.2.1	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
Appendix_II_4.2.1	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.1	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
Appendix_II_4.2.1	<a href="#">secretsmanager-rotation-enabled-check (p. 183)</a>	This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised.
Appendix_II_4.2.1	<a href="#">secretsmanager-scheduled-rotation-success-check (p. 184)</a>	This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised.
Appendix_II_4.2.2	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.2	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
Appendix_II_4.2.2	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
Appendix_II_4.2.2	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
Appendix_II_4.2.2	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

AWS Config Developer Guide  
Operational Best Practices for Esquema  
Nacional de Seguridad (ENS) Low

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.2	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
Appendix_II_4.2.2	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.
Appendix_II_4.2.2	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.4	<a href="#">emr-kerberos-enabled (p. 145)</a>	<p>The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.</p>
Appendix_II_4.2.4	<a href="#">iam-group-has-users-check (p. 153)</a>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.</p>
Appendix_II_4.2.4	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.</p>

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.4	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
Appendix_II_4.2.4	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
Appendix_II_4.2.4	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
Appendix_II_4.2.4	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies.

AWS Config Developer Guide  
Operational Best Practices for Esquema  
Nacional de Seguridad (ENS) Low

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.4	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
Appendix_II_4.2.5	<a href="#">access-keys-rotated (p. 107)</a>	The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.
Appendix_II_4.2.5	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.5	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>
Appendix_II_4.2.5	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.</p>

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.5	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
Appendix_II_4.2.5	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
Appendix_II_4.2.5	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
Appendix_II_4.2.5	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.6	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
Appendix_II_4.2.6	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
Appendix_II_4.2.6	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.6	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
Appendix_II_4.2.6	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
Appendix_II_4.2.6	<a href="#">access-keys-rotated (p. 107)</a>	The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.6	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
Appendix_II_4.2.6	<a href="#">iam-password-policy (p. 154)</a>	The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.6	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
Appendix_II_4.2.6	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
Appendix_II_4.2.6	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
Appendix_II_4.2.6	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.6	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.
Appendix_II_4.2.6	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
Appendix_II_4.2.6	<a href="#">secretsmanager-rotation-enabled-check (p. 183)</a>	This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised.
Appendix_II_4.2.6	<a href="#">secretsmanager-scheduled-rotation-success-check (p. 184)</a>	This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised.

AWS Config Developer Guide  
Operational Best Practices for Esquema  
Nacional de Seguridad (ENS) Low

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.7	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
Appendix_II_4.2.7	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
Appendix_II_4.2.7	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
Appendix_II_4.2.7	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
Appendix_II_4.2.7	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.7	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
Appendix_II_4.2.7	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
Appendix_II_4.2.7	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
Appendix_II_4.2.7	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.7	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
Appendix_II_4.2.7	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
Appendix_II_4.2.7	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
Appendix_II_4.2.7	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.

AWS Config Developer Guide  
Operational Best Practices for Esquema  
Nacional de Seguridad (ENS) Low

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.7	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
Appendix_II_4.2.7	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
Appendix_II_4.2.7	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
Appendix_II_4.2.7	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.7	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
Appendix_II_4.2.7	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.
Appendix_II_4.2.7	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
Appendix_II_4.2.7	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.7	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
Appendix_II_4.2.7	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
Appendix_II_4.2.7	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
Appendix_II_4.2.7	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.3.1	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
Appendix_II_4.3.1	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
Appendix_II_4.3.1	<a href="#">ec2-security-group-attached-to-eni (p. 137)</a>	This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment.
Appendix_II_4.3.1	<a href="#">eip-attached (p. 139)</a>	This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.3.2	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
Appendix_II_4.3.2	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
Appendix_II_4.3.4	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
Appendix_II_4.3.4	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.3.4	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
Appendix_II_4.3.4	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
Appendix_II_4.3.6	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
Appendix_II_4.3.6	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.3.8	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
Appendix_II_4.3.8	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
Appendix_II_4.3.8	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.3.8	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
Appendix_II_4.3.11	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.
Appendix_II_4.3.11	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
Appendix_II_4.3.11	<a href="#">alb-http-to-https-redirection-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
Appendix_II_4.3.11	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
Appendix_II_4.3.11	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.3.11	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
Appendix_II_4.3.11	<a href="#">cmk-backing-key-rotation-enabled (p. 123)</a>	Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period.
Appendix_II_4.3.11	<a href="#">dynamodb-table-encrypted-kms (p. 129)</a>	Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK).
Appendix_II_4.3.11	<a href="#">ec2-efs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
Appendix_II_4.3.11	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
Appendix_II_4.3.11	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
Appendix_II_4.3.11	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.3.11	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
Appendix_II_4.3.11	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
Appendix_II_4.3.11	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
Appendix_II_4.3.11	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.
Appendix_II_4.3.11	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.
Appendix_II_4.3.11	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.3.11	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
Appendix_II_4.3.11	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
Appendix_II_4.3.11	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
Appendix_II_4.3.11	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
Appendix_II_4.3.11	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.3.11	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.
Appendix_II_4.3.11	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.
Appendix_II_4.6.2	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
Appendix_II_4.6.2	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.6.2	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
Appendix_II_4.6.2	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
Appendix_II_4.6.2	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
Appendix_II_4.6.2	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.6.2	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	<p>AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.</p>
Appendix_II_4.6.2	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	<p>Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.</p>
Appendix_II_4.6.2	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	<p>The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.</p>

Control ID	AWS Config Rule	Guidance
Appendix_II_5.4.1	<a href="#">alb-waf-enabled (p. 109)</a>	Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.
Appendix_II_5.4.1	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
Appendix_II_5.4.1	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
Appendix_II_5.4.1	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
Appendix_II_5.4.1	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

AWS Config Developer Guide  
Operational Best Practices for Esquema  
Nacional de Seguridad (ENS) Low

Control ID	AWS Config Rule	Guidance
Appendix_II_5.4.1	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
Appendix_II_5.4.1	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
Appendix_II_5.4.1	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
Appendix_II_5.4.1	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	AWS Config Rule	Guidance
Appendix_II_5.4.1	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
Appendix_II_5.4.1	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
Appendix_II_5.4.1	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
Appendix_II_5.4.1	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
Appendix_II_5.4.1	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
Appendix_II_5.4.1	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
Appendix_II_5.4.1	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
Appendix_II_5.4.1	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	AWS Config Rule	Guidance
Appendix_II_5.4.1	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
Appendix_II_5.4.1	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
Appendix_II_5.4.1	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
Appendix_II_5.4.3	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.
Appendix_II_5.4.3	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
Appendix_II_5.4.3	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
Appendix_II_5.4.3	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
Appendix_II_5.4.3	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
Appendix_II_5.4.3	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
Appendix_II_5.4.3	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
Appendix_II_5.4.3	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
Appendix_II_5.4.3	<a href="#">rds-snapshots-public-prohibited</a> (p. 168)	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
Appendix_II_5.4.3	<a href="#">redshift-cluster-public-access-check</a> (p. 171)	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
Appendix_II_5.4.3	<a href="#">restricted-common-ports</a> (p. 174)	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
Appendix_II_5.4.3	<a href="#">s3-account-level-public-access-blocks</a> (p. 175)	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
Appendix_II_5.4.3	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
Appendix_II_5.4.3	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
Appendix_II_5.4.3	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
Appendix_II_5.5.3	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
Appendix_II_5.5.3	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
Appendix_II_5.5.3	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
Appendix_II_5.5.3	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
Appendix_II_5.5.3	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
Appendix_II_5.5.3	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
Appendix_II_5.5.3	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
Appendix_II_5.5.3	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
Appendix_II_5.5.3	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.
Appendix_II_5.5.3	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
Appendix_II_5.5.3	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	AWS Config Rule	Guidance
Appendix_II_5.6.2	<a href="#">codebuild-project-envvar-awscred-check (p. 123)</a>	Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access.
Appendix_II_5.6.2	<a href="#">codebuild-project-source-repo-url-check (p. 123)</a>	Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, user name and password within AWS Codebuild project environments. Use OAuth instead of personal access tokens or a user name and password to grant authorization for accessing GitHub or Bitbucket repositories.
Appendix_II_5.7.1	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non- repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
Appendix_II_5.7.1	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.

AWS Config Developer Guide  
Operational Best Practices for Esquema  
Nacional de Seguridad (ENS) Low

Control ID	AWS Config Rule	Guidance
Appendix_II_5.7.1	<a href="#">codebuild-project-envvar-awscred-check (p. 123)</a>	Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access.
Appendix_II_5.7.1	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
Appendix_II_5.7.1	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
Appendix_II_5.7.1	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
Appendix_II_5.7.1	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

AWS Config Developer Guide  
Operational Best Practices for Esquema  
Nacional de Seguridad (ENS) Low

Control ID	AWS Config Rule	Guidance
Appendix_II_5.7.1	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
Appendix_II_5.7.1	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
Appendix_II_5.7.1	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
Appendix_II_5.7.1	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
Appendix_II_5.7.1	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
Appendix_II_5.7.1	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
Appendix_II_5.7.1	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
Appendix_II_5.7.1	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	AWS Config Rule	Guidance
Appendix_II_5.7.1	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
Appendix_II_5.7.1	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
Appendix_II_5.7.1	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
Appendix_II_5.7.1	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
Appendix_II_5.7.4	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
Appendix_II_5.7.4	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
Appendix_II_5.7.7	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.
Appendix_II_5.7.7	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.
Appendix_II_5.7.7	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
Appendix_II_5.7.7	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.

Control ID	AWS Config Rule	Guidance
Appendix_II_5.7.7	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.
Appendix_II_5.8.2	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
Appendix_II_5.8.2	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.

## Template

The template is available on GitHub: [Operational Best Practices for Esquema Nacional de Seguridad \(ENS\) Low](#).

## Operational Best Practices for Esquema Nacional de Seguridad (ENS) Medium

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between Spain Esquema Nacional de Seguridad (ENS) Medium framework controls and AWS managed Config rules. Each Config rule applies to a specific AWS resource,

and relates to one or more Spain ENS Medium controls. A Spain ENS control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This sample conformance pack template contains mappings to controls within the Spain ENS Medium framework, as last updated on 2020/10/23.

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

Control ID	AWS Config Rule	Guidance
Article_16	<a href="#">access-keys-rotated (p. 107)</a>	The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.
Article_16	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
Article_16	<a href="#">iam-password-policy (p. 154)</a>	The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS

Control ID	AWS Config Rule	Guidance
		<p>Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>
Article_16	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.</p>
Article_16	<a href="#">iam-root-access-key-check (p. 157)</a>	<p>Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.</p>
Article_16	<a href="#">iam-user-group-membership-check (p. 157)</a>	<p>AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.</p>

Control ID	AWS Config Rule	Guidance
Article_16	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
Article_16	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.
Article_16	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
Article_16	<a href="#">secretsmanager-rotation-enabled-check (p. 183)</a>	This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised.

Control ID	AWS Config Rule	Guidance
Article_20	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
Article_20	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
Article_20	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
Article_21	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
Article_21	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
Article_21	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.

Control ID	AWS Config Rule	Guidance
Article_21	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
Article_21	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
Article_21	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
Article_21	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.
Article_21	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.
Article_21	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.
Article_21	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.

Control ID	AWS Config Rule	Guidance
Article_21	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.
Article_21	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.
Article_21	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.
Article_21	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
Article_21	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
Article_21	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	AWS Config Rule	Guidance
Article_21	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
Article_22	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
Article_22	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
Article_22	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.

Control ID	AWS Config Rule	Guidance
Article_22	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
Article_22	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
Article_22	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
Article_22	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
Article_22	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
Article_23	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
Article_23	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	AWS Config Rule	Guidance
Article_23	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
Article_23	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
Article_23	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
Article_23	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.

Control ID	AWS Config Rule	Guidance
Article_23	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.
Article_23	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
Article_23	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.

Control ID	AWS Config Rule	Guidance
Article_24	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
Article_24	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
Article_24	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
Article_24	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	AWS Config Rule	Guidance
Article_24	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.
Article_24	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
Article_24	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	AWS Config Rule	Guidance
Article_24	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
Article_24	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment.
Article_24	<a href="#">codebuild-project-source-repo-url-check (p. 123)</a>	Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, user name and password within AWS Codebuild project environments. Use OAuth instead of personal access tokens or a user name and password to grant authorization for accessing GitHub or Bitbucket repositories.
Article_24	<a href="#">lambda-dlq-check (p. 161)</a>	Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed.

Control ID	AWS Config Rule	Guidance
Article_25	<a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a>	The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.
Article_25	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.
Article_25	<a href="#">dynamodb-autoscaling-enabled (p. 128)</a>	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.

Control ID	AWS Config Rule	Guidance
Article_25	<a href="#">dynamodb-throughput-limit-check (p. 130)</a>	Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set <code>accountRCUThresholdPercentage</code> (Config Default: 80) and <code>accountWCUThresholdPercentage</code> (Config Default: 80) parameters. The actual values should reflect your organization's policies.
Article_25	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
Article_25	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.

Control ID	AWS Config Rule	Guidance
Article_25	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
Article_25	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
Article_25	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.

Control ID	AWS Config Rule	Guidance
Article_25	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.
Article_25	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.
Article_31	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
Article_31	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
Article_31	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	AWS Config Rule	Guidance
Article_31	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
Article_31	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
Article_31	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	AWS Config Rule	Guidance
Article_31	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
Article_33	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
Article_33	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.
Article_35	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	AWS Config Rule	Guidance
Article_35	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
Article_37	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
Article_37	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
Article_37	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
Article_37	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.

Control ID	AWS Config Rule	Guidance
Article_37	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
Article_37	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
Article_37	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
Article_37	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
Article_37	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
Article_37	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
Article_37	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.

Control ID	AWS Config Rule	Guidance
Article_37	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
Article_37	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
Article_37	<a href="#">codebuild-project-source-repo-url-check (p. 123)</a>	Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, user name and password within AWS Codebuild project environments. Use OAuth instead of personal access tokens or a user name and password to grant authorization for accessing GitHub or Bitbucket repositories.
Article_37	<a href="#">lambda-dlq-check (p. 161)</a>	Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.1	<a href="#">access-keys-rotated (p. 107)</a>	The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.
Appendix_II_4.2.1	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.1	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>
Appendix_II_4.2.1	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.</p>

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.1	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
Appendix_II_4.2.1	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
Appendix_II_4.2.1	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
Appendix_II_4.2.1	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.1	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
Appendix_II_4.2.1	<a href="#">secretsmanager-rotation-enabled-check (p. 183)</a>	This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised.
Appendix_II_4.2.1	<a href="#">secretsmanager-scheduled-rotation-success-check (p. 184)</a>	This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised.
Appendix_II_4.2.2	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.2	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
Appendix_II_4.2.2	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
Appendix_II_4.2.2	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
Appendix_II_4.2.2	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.2	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
Appendix_II_4.2.2	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.
Appendix_II_4.2.2	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.3	<a href="#">emr-kerberos-enabled (p. 145)</a>	<p>The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.</p>
Appendix_II_4.2.3	<a href="#">iam-group-has-users-check (p. 153)</a>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.</p>
Appendix_II_4.2.3	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.</p>

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.3	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
Appendix_II_4.2.3	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
Appendix_II_4.2.3	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
Appendix_II_4.2.3	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.3	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
Appendix_II_4.2.4	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
Appendix_II_4.2.4	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.4	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
Appendix_II_4.2.4	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
Appendix_II_4.2.4	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
Appendix_II_4.2.4	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.4	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.
Appendix_II_4.2.4	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
Appendix_II_4.2.5	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
Appendix_II_4.2.5	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.5	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
Appendix_II_4.2.5	<a href="#">access-keys-rotated (p. 107)</a>	The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.
Appendix_II_4.2.5	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.5	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>
Appendix_II_4.2.5	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.</p>

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.5	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
Appendix_II_4.2.5	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
Appendix_II_4.2.5	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
Appendix_II_4.2.5	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.6	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
Appendix_II_4.2.6	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
Appendix_II_4.2.6	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.6	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
Appendix_II_4.2.6	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
Appendix_II_4.2.6	<a href="#">access-keys-rotated (p. 107)</a>	The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.6	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
Appendix_II_4.2.6	<a href="#">iam-password-policy (p. 154)</a>	The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.6	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
Appendix_II_4.2.6	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
Appendix_II_4.2.6	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
Appendix_II_4.2.6	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.6	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.
Appendix_II_4.2.6	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
Appendix_II_4.2.6	<a href="#">secretsmanager-rotation-enabled-check (p. 183)</a>	This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised.
Appendix_II_4.2.6	<a href="#">secretsmanager-scheduled-rotation-success-check (p. 184)</a>	This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.7	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
Appendix_II_4.2.7	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
Appendix_II_4.2.7	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
Appendix_II_4.2.7	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
Appendix_II_4.2.7	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.7	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
Appendix_II_4.2.7	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
Appendix_II_4.2.7	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
Appendix_II_4.2.7	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.7	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
Appendix_II_4.2.7	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
Appendix_II_4.2.7	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
Appendix_II_4.2.7	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.7	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
Appendix_II_4.2.7	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
Appendix_II_4.2.7	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
Appendix_II_4.2.7	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.7	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
Appendix_II_4.2.7	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.
Appendix_II_4.2.7	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
Appendix_II_4.2.7	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.2.7	<a href="#">s3-bucket-public-write-prohibited</a> (p. 180)	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
Appendix_II_4.2.7	<a href="#">sagemaker-notebook-no-direct-internet-access</a> (p. 183)	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
Appendix_II_4.2.7	<a href="#">vpc-default-security-group-closed</a> (p. 188)	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
Appendix_II_4.2.7	<a href="#">vpc-sg-open-only-to-authorized-ports</a> (p. 189)	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.3.1	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
Appendix_II_4.3.1	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
Appendix_II_4.3.1	<a href="#">ec2-security-group-attached-to-eni (p. 137)</a>	This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment.
Appendix_II_4.3.1	<a href="#">eip-attached (p. 139)</a>	This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.3.2	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
Appendix_II_4.3.2	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
Appendix_II_4.3.3	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
Appendix_II_4.3.3	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.3.3	<a href="#">ec2-stopped-instance (p. 137)</a>	Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards.
Appendix_II_4.3.3	<a href="#">ec2-volume-inuse-check (p. 137)</a>	This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality.
Appendix_II_4.3.4	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
Appendix_II_4.3.4	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.3.4	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
Appendix_II_4.3.4	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
Appendix_II_4.3.6	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
Appendix_II_4.3.6	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.3.7	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
Appendix_II_4.3.7	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
Appendix_II_4.3.7	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
Appendix_II_4.3.7	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
Appendix_II_4.3.7	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.3.7	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
Appendix_II_4.3.7	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
Appendix_II_4.3.7	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.3.7	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
Appendix_II_4.3.7	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
Appendix_II_4.3.7	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.3.7	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.
Appendix_II_4.3.7	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
Appendix_II_4.3.7	<a href="#">codebuild-project-source-repo-url-check (p. 123)</a>	Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, user name and password within AWS Codebuild project environments. Use OAuth instead of personal access tokens or a user name and password to grant authorization for accessing GitHub or Bitbucket repositories.
Appendix_II_4.3.7	<a href="#">lambda-dlq-check (p. 161)</a>	Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.3.8	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
Appendix_II_4.3.8	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
Appendix_II_4.3.8	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.3.8	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
Appendix_II_4.3.9	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
Appendix_II_4.3.9	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
Appendix_II_4.3.9	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
Appendix_II_4.3.9	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.3.9	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
Appendix_II_4.3.9	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
Appendix_II_4.3.9	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
Appendix_II_4.3.9	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.3.9	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
Appendix_II_4.3.9	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
Appendix_II_4.3.9	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.3.9	<a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a>	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.
Appendix_II_4.3.11	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.
Appendix_II_4.3.11	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
Appendix_II_4.3.11	<a href="#">alb-http-to-https-redirection-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
Appendix_II_4.3.11	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
Appendix_II_4.3.11	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.3.11	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
Appendix_II_4.3.11	<a href="#">cmk-backing-key-rotation-enabled (p. 123)</a>	Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period.
Appendix_II_4.3.11	<a href="#">dynamodb-table-encrypted-kms (p. 129)</a>	Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK).
Appendix_II_4.3.11	<a href="#">ec2-ebs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
Appendix_II_4.3.11	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
Appendix_II_4.3.11	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
Appendix_II_4.3.11	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.3.11	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
Appendix_II_4.3.11	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
Appendix_II_4.3.11	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
Appendix_II_4.3.11	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.
Appendix_II_4.3.11	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.
Appendix_II_4.3.11	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.3.11	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
Appendix_II_4.3.11	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
Appendix_II_4.3.11	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
Appendix_II_4.3.11	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
Appendix_II_4.3.11	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.3.11	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.
Appendix_II_4.3.11	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.
Appendix_II_4.4.2	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
Appendix_II_4.4.2	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.4.2	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
Appendix_II_4.6.1	<a href="#">alb-waf-enabled (p. 109)</a>	Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.
Appendix_II_4.6.1	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
Appendix_II_4.6.1	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.6.1	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
Appendix_II_4.6.1	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
Appendix_II_4.6.1	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
Appendix_II_4.6.2	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.6.2	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
Appendix_II_4.6.2	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
Appendix_II_4.6.2	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
Appendix_II_4.6.2	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
Appendix_II_4.6.2	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	AWS Config Rule	Guidance
Appendix_II_4.6.2	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	<p>AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.</p>
Appendix_II_4.6.2	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	<p>Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.</p>
Appendix_II_4.6.2	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	<p>The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.</p>

Control ID	AWS Config Rule	Guidance
Appendix_II_5.4.1	<a href="#">alb-waf-enabled (p. 109)</a>	Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.
Appendix_II_5.4.1	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
Appendix_II_5.4.1	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
Appendix_II_5.4.1	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
Appendix_II_5.4.1	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
Appendix_II_5.4.1	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
Appendix_II_5.4.1	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
Appendix_II_5.4.1	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
Appendix_II_5.4.1	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	AWS Config Rule	Guidance
Appendix_II_5.4.1	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
Appendix_II_5.4.1	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
Appendix_II_5.4.1	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
Appendix_II_5.4.1	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
Appendix_II_5.4.1	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
Appendix_II_5.4.1	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
Appendix_II_5.4.1	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
Appendix_II_5.4.1	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	AWS Config Rule	Guidance
Appendix_II_5.4.1	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
Appendix_II_5.4.1	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
Appendix_II_5.4.1	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
Appendix_II_5.4.2	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.

Control ID	AWS Config Rule	Guidance
Appendix_II_5.4.2	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
Appendix_II_5.4.2	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
Appendix_II_5.4.2	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.

Control ID	AWS Config Rule	Guidance
Appendix_II_5.4.2	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
Appendix_II_5.4.2	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
Appendix_II_5.4.2	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
Appendix_II_5.4.2	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.

Control ID	AWS Config Rule	Guidance
Appendix_II_5.4.3	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.
Appendix_II_5.4.3	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
Appendix_II_5.4.3	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
Appendix_II_5.4.3	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
Appendix_II_5.4.3	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.

Control ID	AWS Config Rule	Guidance
Appendix_II_5.4.3	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
Appendix_II_5.4.3	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
Appendix_II_5.4.3	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
Appendix_II_5.4.3	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	AWS Config Rule	Guidance
Appendix_II_5.4.3	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
Appendix_II_5.4.3	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
Appendix_II_5.4.3	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
Appendix_II_5.4.3	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
Appendix_II_5.4.3	<a href="#">restricted-common-ports</a> (p. 174)	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
Appendix_II_5.4.3	<a href="#">s3-account-level-public-access-blocks</a> (p. 175)	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
Appendix_II_5.4.3	<a href="#">s3-bucket-public-read-prohibited</a> (p. 179)	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
Appendix_II_5.4.3	<a href="#">s3-bucket-public-write-prohibited</a> (p. 180)	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	AWS Config Rule	Guidance
Appendix_II_5.4.3	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
Appendix_II_5.4.3	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
Appendix_II_5.4.3	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
Appendix_II_5.5.3	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
Appendix_II_5.5.3	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
Appendix_II_5.5.3	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
Appendix_II_5.5.3	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
Appendix_II_5.5.3	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
Appendix_II_5.5.3	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
Appendix_II_5.5.3	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
Appendix_II_5.5.3	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
Appendix_II_5.5.3	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
Appendix_II_5.5.3	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
Appendix_II_5.5.3	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	AWS Config Rule	Guidance
Appendix_II_5.6.1	<a href="#">codebuild-project-envvar-awscred-check (p. 123)</a>	Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access.
Appendix_II_5.6.1	<a href="#">codebuild-project-source-repo-url-check (p. 123)</a>	Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, user name and password within AWS Codebuild project environments. Use OAuth instead of personal access tokens or a user name and password to grant authorization for accessing GitHub or Bitbucket repositories.
Appendix_II_5.6.2	<a href="#">codebuild-project-envvar-awscred-check (p. 123)</a>	Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access.
Appendix_II_5.6.2	<a href="#">codebuild-project-source-repo-url-check (p. 123)</a>	Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, user name and password within AWS Codebuild project environments. Use OAuth instead of personal access tokens or a user name and password to grant authorization for accessing GitHub or Bitbucket repositories.

Control ID	AWS Config Rule	Guidance
Appendix_II_5.6.2	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
Appendix_II_5.6.2	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
Appendix_II_5.7.1	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
Appendix_II_5.7.1	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.

Control ID	AWS Config Rule	Guidance
Appendix_II_5.7.1	<a href="#">codebuild-project-envvar-awscred-check (p. 123)</a>	Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access.
Appendix_II_5.7.1	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
Appendix_II_5.7.1	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
Appendix_II_5.7.1	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
Appendix_II_5.7.1	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	AWS Config Rule	Guidance
Appendix_II_5.7.1	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
Appendix_II_5.7.1	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
Appendix_II_5.7.1	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
Appendix_II_5.7.1	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
Appendix_II_5.7.1	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
Appendix_II_5.7.1	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
Appendix_II_5.7.1	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
Appendix_II_5.7.1	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	AWS Config Rule	Guidance
Appendix_II_5.7.1	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
Appendix_II_5.7.1	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
Appendix_II_5.7.1	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
Appendix_II_5.7.1	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
Appendix_II_5.7.4	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
Appendix_II_5.7.4	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
Appendix_II_5.7.7	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.
Appendix_II_5.7.7	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.
Appendix_II_5.7.7	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
Appendix_II_5.7.7	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.

Control ID	AWS Config Rule	Guidance
Appendix_II_5.7.7	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.
Appendix_II_5.8.2	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
Appendix_II_5.8.2	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.

## Template

The template is available on GitHub: [Operational Best Practices for Esquema Nacional de Seguridad \(ENS\) Medium](#).

# Operational Best Practices for FDA Title 21 CFR Part 11

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Title 21 of the Code of Federal Regulations (CFR) Part 11 and AWS managed Config rules. Each AWS Config rule applies to a specific AWS resource, and relates to one or more FDA Title 21 CFR Part 11 controls. A FDA Title 21 CFR Part 11 control can be

related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This Conformance Pack was validated by AWS Security Assurance Services LLC (AWS SAS), which is a team of Payment Card Industry Qualified Security Assessors (QSAs), HITRUST Certified Common Security Framework Practitioners (CCSFPs), and compliance professionals certified to provide guidance and assessments for various industry frameworks. AWS SAS professionals designed this Conformance Pack to enable you to align to a subset of FDA Title 21 CFR Part 11 design principles.

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

Control ID	Control Description	AWS Config Rule	Guidance
11.10(a)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.
11.10(a)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a)	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.		
11.10(a)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	<a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a>	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(a)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.</p>	<p><a href="#">db-instance-backup-enabled (p. 126)</a></p>	<p>The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.</p>
11.10(a)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.</p>	<p><a href="#">dynamodb-autoscaling-enabled (p. 128)</a></p>	<p>Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(a)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.</p>	<p><a href="#">dynamodb-in-backup-plan (p. 128)</a></p>	<p>To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.</p>
11.10(a)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.</p>	<p><a href="#">dynamodb-pitr-enabled (p. 129)</a></p>	<p>Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(a)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.</p>	<p><a href="#">ebs-in-backup-plan (p. 130)</a></p>	<p>To help with data backup processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.</p>
11.10(a)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.</p>	<p><a href="#">ebs-optimized-instance (p. 131)</a></p>	<p>An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(a)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.</p>	<p><a href="#">efs-in-backup-plan (p. 139)</a></p>	<p>To help with data backup processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.</p>
11.10(a)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.</p>	<p><a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a></p>	<p>When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(a)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.</p>	<p><a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a></p>	<p>Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.</p>
11.10(a)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.</p>	<p><a href="#">elb-deletion-protection-enabled (p. 144)</a></p>	<p>This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(a)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.</p>	<p><a href="#">rds-in-backup-plan (p. 167)</a></p>	<p>To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.</p>
11.10(a)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.</p>	<p><a href="#">rds-instance-deletion-protection-enabled (p. 166)</a></p>	<p>Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(a)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.</p>	<a href="#">rds-multi-az-support (p. 168)</a>	<p>Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(a)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.</p>	<p><a href="#">s3-bucket-replication-enabled (p. 180)</a></p>	<p>Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.</p>
11.10(a)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.</p>	<p><a href="#">vpc-vpn-2-tunnels-up (p. 189)</a></p>	<p>Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(a)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.</p>	<p><a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a></p>	<p>An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.</p>
11.10(a)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.</p>	<p><a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a></p>	<p>Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(a)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.</p>	<p><a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a></p>	<p>Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.</p>
11.10(a)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.</p>	<p><a href="#">ec2-stopped-instance (p. 137)</a></p>	<p>Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(a)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.</p>	<p><a href="#">ec2-volume-inuse-check (p. 137)</a></p>	<p>This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality.</p>
11.10(c)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.</p>	<p><a href="#">s3-bucket-public-read-prohibited (p. 179)</a></p>	<p>Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(c)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.</p>	<p><a href="#">cw-loggroup-retention-period-check (p. 125)</a></p>	<p>Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events.</p>
11.10(c)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.</p>	<p><a href="#">s3-bucket-public-write-prohibited (p. 180)</a></p>	<p>Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(c)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.</p>	<p><a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a></p>	<p>To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.</p>
11.10(c)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.</p>	<p><a href="#">s3-bucket-ssl-requests-only (p. 181)</a></p>	<p>To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(c)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.</p>	<p><a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a></p>	<p>To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.</p>
11.10(c)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.</p>	<p><a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a></p>	<p>To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(c)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.</p>	<p><a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.</p>
11.10(c)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.</p>	<p><a href="#">redshift-cluster-public-access-check (p. 171)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(c)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.</p>	<p><a href="#">redshift-require-tls-ssl (p. 172)</a></p>	<p>Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.</p>
11.10(c)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.</p>	<p><a href="#">redshift-cluster-configuration-check (p. 170)</a></p>	<p>To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(c)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.</p>	<p><a href="#">rds-snapshot-encrypted (p. 168)</a></p>	<p>Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.</p>
11.10(c)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.</p>	<p><a href="#">rds-snapshots-public-prohibited (p. 168)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(c)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.</p>	<p><a href="#">rds-storage-encrypted (p. 169)</a></p>	<p>To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.</p>
11.10(c)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.</p>	<p><a href="#">s3-bucket-versioning-enabled (p. 181)</a></p>	<p>Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<p><a href="#">access-keys-rotated (p. 107)</a></p>	<p>The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.</p>
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<p><a href="#">ec2-imdsv2-check (p. 132)</a></p>	<p>Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<p><a href="#">emr-kerberos-enabled (p. 145)</a></p>	<p>The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.</p>
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<p><a href="#">iam-group-has-users-check (p. 153)</a></p>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(d)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals.	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<p><a href="#">iam-password-policy</a> (p. 154)</p>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<p><a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a></p>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.</p>
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<p><a href="#">iam-root-access-key-check (p. 157)</a></p>	<p>Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<p><a href="#">iam-user-group-membership-check (p. 157)</a></p>	<p>AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.</p>
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<p><a href="#">iam-user-mfa-enabled (p. 158)</a></p>	<p>Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<p><a href="#">iam-user-no-policies-check (p. 158)</a></p>	<p>This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.</p>
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<p><a href="#">iam-user-unused-credentials-check (p. 159)</a></p>	<p>AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<p><a href="#">mfa-enabled-for-iam-console-access (p. 163)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.</p>
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<p><a href="#">root-account-hardware-mfa-enabled (p. 175)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<a href="#">root-account-mfa-enabled (p. 175)</a>	<p>Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.</p>
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	<p>Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code>. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<p><a href="#">secretsmanager-rotation-enabled-check (p. 183)</a></p>	<p>This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised.</p>
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<p><a href="#">secretsmanager-scheduled-rotation-success-check (p. 184)</a></p>	<p>This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<p><a href="#">dms-replication-not-public (p. 127)</a></p>	<p>Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.</p>
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<p><a href="#">ebs-snapshot-public-restorable-check (p. 131)</a></p>	<p>Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<p><a href="#">ec2-instance-no-public-ip (p. 133)</a></p>	<p>Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.</p>
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<p><a href="#">elasticsearch-in-vpc-only (p. 141)</a></p>	<p>Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<p><a href="#">emr-master-no-public-ip (p. 146)</a></p>	<p>Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.</p>
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<p><a href="#">restricted-ssh (p. 159)</a></p>	<p>Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<p><a href="#">ec2-instances-in-vpc (p. 159)</a></p>	<p>Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.</p>
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<p><a href="#">internet-gateway-authorized-vpc-only (p. 160)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<p><a href="#">lambda-function-public-access-prohibited (p. 161)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.</p>
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<p><a href="#">lambda-inside-vpc (p. 162)</a></p>	<p>Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<p><a href="#">rds-instance-public-access-check (p. 166)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.</p>
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<p><a href="#">restricted-common-ports (p. 174)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<p><a href="#">s3-account-level-public-access-blocks (p. 175)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.</p>
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<p><a href="#">vpc-default-security-group-closed (p. 188)</a></p>	<p>Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<p><a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.</p>
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<p><a href="#">rds-snapshots-public-prohibited (p. 168)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<p><a href="#">redshift-cluster-public-access-check (p. 171)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.</p>
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<p><a href="#">s3-bucket-public-read-prohibited (p. 179)</a></p>	<p>Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<p><a href="#">s3-bucket-public-write-prohibited (p. 180)</a></p>	<p>Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.</p>
11.10(d)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p> <p>(d) Limiting system access to authorized individuals.</p>	<p><a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(e)	(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
11.10(e)	(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(e)	(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
11.10(e)	(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(e)	(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
11.10(e)	(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(e)	(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
11.10(e)	(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(e)	(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
11.10(e)	(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(e)	(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	<a href="#">cw-loggroup-retention-period-check (p. 125)</a>	Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events.
11.10(e)	(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.</p>	<p><a href="#">elasticsearch-encrypted-at-rest (p. 141)</a></p>	<p>Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">ec2-ebs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.</p>	<a href="#">dynamodb-table-encrypted-kms (p. 129)</a>	<p>Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK).</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">access-keys-rotated (p. 107)</a>	The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.</p>	<a href="#">ec2-imsdv2-check (p. 132)</a>	<p>Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.</p>	<p><a href="#">iam-password-policy (p. 154)</a></p>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.</p>	<a href="#">iam-root-access-key-check (p. 157)</a>	<p>Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.</p>	<p><a href="#">secretsmanager-rotation-enabled-check (p. 183)</a></p>	<p>This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.</p>	<p><a href="#">secretsmanager-scheduled-rotation-success-check (p. 184)</a></p>	<p>This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(g)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.</p>	<p><a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.</p>
11.10(h)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.</p>	<p><a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a></p>	<p>An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(h)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.</p>	<p><a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a></p>	<p>Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.</p>
11.10(h)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.</p>	<p><a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a></p>	<p>Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(k)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(k)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.</p>	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	<p>Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(k)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.</p>	<a href="#">emr-master-no-public-ip (p. 146)</a>	<p>Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(k)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(k)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.</p>	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	<p>Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(k)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.</p>	<a href="#">rds-instance-public-access-check (p. 166)</a>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(k)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(k)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.</p>	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(k)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(k)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.</p>	<p><a href="#">s3-account-level-public-access-blocks (p. 175)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(k)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(k)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.</p>	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	<p>Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(k)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(k)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(k)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(k)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.</p>	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	<p>Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.10(k)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(k)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(k)	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.

Control ID	Control Description	AWS Config Rule	Guidance
11.10(k)	<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.</p>	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	<p>Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.30	Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	<a href="#">dynamodb-table-encrypted-kms (p. 129)</a>	Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK).

Control ID	Control Description	AWS Config Rule	Guidance
11.30	Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	<a href="#">ec2-ebs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
11.30	Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).

Control ID	Control Description	AWS Config Rule	Guidance
11.30	Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.

Control ID	Control Description	AWS Config Rule	Guidance
11.30	Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
11.30	Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.

Control ID	Control Description	AWS Config Rule	Guidance
11.30	Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
11.30	Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
11.30	Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
11.30	Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
11.30	Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
11.30	Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
11.30	Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
11.30	Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
11.30	Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	<a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a>	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.

Control ID	Control Description	AWS Config Rule	Guidance
11.30	Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.

Control ID	Control Description	AWS Config Rule	Guidance
11.30	Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	<a href="#">cmk-backing-key-rotation-enabled (p. 123)</a>	Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period.

Control ID	Control Description	AWS Config Rule	Guidance
11.30	Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.

Control ID	Control Description	AWS Config Rule	Guidance
11.30	Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
11.30	Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.

Control ID	Control Description	AWS Config Rule	Guidance
11.30	Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
11.200	<p>(a) Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password. (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components. (2) Be used only by their genuine owners; and (3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.</p>	<p><a href="#">access-keys-rotated (p. 107)</a></p>	<p>The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.200	<p>(a) Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password. (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components. (2) Be used only by their genuine owners; and (3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.</p>	<p><a href="#">iam-password-policy (p. 154)</a></p>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.200	<p>(a) Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password. (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components. (2) Be used only by their genuine owners; and (3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.</p>	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.

Control ID	Control Description	AWS Config Rule	Guidance
11.200	<p>(a) Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password. (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components. (2) Be used only by their genuine owners; and (3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.</p>	<p><a href="#">iam-user-mfa-enabled (p. 158)</a></p>	<p>Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.200	<p>(a) Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password. (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components. (2) Be used only by their genuine owners; and (3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.</p>	<p><a href="#">mfa-enabled-for-iam-console-access (p. 163)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.200	<p>(a) Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password. (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components. (2) Be used only by their genuine owners; and (3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.</p>	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	<p>Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.200	<p>(a) Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password. (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components. (2) Be used only by their genuine owners; and (3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.</p>	<p><a href="#">root-account-mfa-enabled (p. 175)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.300(b)	<p>Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:</p> <p>(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).</p>	<p><a href="#">iam-password-policy (p. 154)</a></p>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.300(b)	Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include: (b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	<a href="#">access-keys-rotated (p. 107)</a>	The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
11.300(b)	Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include: (b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.

Control ID	Control Description	AWS Config Rule	Guidance
11.300(b)	<p>Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:</p> <p>(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).</p>	<p><a href="#">iam-user-unused-credentials-check (p. 159)</a></p>	<p>AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.</p>
11.300(b)	<p>Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:</p> <p>(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).</p>	<p><a href="#">secretsmanager-rotation-enabled-check (p. 183)</a></p>	<p>This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.300(b)	<p>Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:</p> <p>(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).</p>	<p><a href="#">secretsmanager-scheduled-rotation-success-check</a> (p. 184)</p>	<p>This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised.</p>
11.300(d)	<p>Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include: (d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.</p>	<p><a href="#">cloud-trail-cloud-watch-logs-enabled</a> (p. 121)</p>	<p>Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.300(d)	<p>Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include: (d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.</p>	<p><a href="#">cloudtrail-enabled (p. 121)</a></p>	<p>AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.</p>
11.300(d)	<p>Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include: (d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.</p>	<p><a href="#">securityhub-enabled (p. 186)</a></p>	<p>AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.</p>

Control ID	Control Description	AWS Config Rule	Guidance
11.300(d)	Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include: (d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

## Template

The template is available on GitHub: [Operational Best Practices for FDA Title 21 CFR Part 11](#).

## Operational Best Practices for FedRAMP(Low)

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Federal Risk and Authorization Management Program (FedRAMP) Low Baseline Controls and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more FedRAMP controls. A FedRAMP control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

Control ID	Control Description	AWS Config Rule	Guidance
AC-2	ACCOUNT MANAGEMENT	<a href="#">secretsmanager-scheduled-rotation-success-check (p. 184)</a>	This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the

Control ID	Control Description	AWS Config Rule	Guidance
			<p>rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised.</p>
AC-2	ACCOUNT MANAGEMENT	iam-password-policy (p. 154)	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AC-2	ACCOUNT MANAGEMENT	<a href="#">access-keys-rotated (p. 107)</a>	The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.
AC-2	ACCOUNT MANAGEMENT	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AC-2	ACCOUNT MANAGEMENT	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC-2	ACCOUNT MANAGEMENT	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
AC-2	ACCOUNT MANAGEMENT	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
AC-2	ACCOUNT MANAGEMENT	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
AC-2	ACCOUNT MANAGEMENT	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
AC-2	ACCOUNT MANAGEMENT	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.

Control ID	Control Description	AWS Config Rule	Guidance
AC-2	ACCOUNT MANAGEMENT	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
AC-2	ACCOUNT MANAGEMENT	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), and <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.

Control ID	Control Description	AWS Config Rule	Guidance
AC-2	ACCOUNT MANAGEMENT	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.
AC-2	ACCOUNT MANAGEMENT	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.

Control ID	Control Description	AWS Config Rule	Guidance
AC-2	ACCOUNT MANAGEMENT	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
AC-2	ACCOUNT MANAGEMENT	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
AC-2	ACCOUNT MANAGEMENT	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC-2	ACCOUNT MANAGEMENT	<a href="#">emr-kerberos-enabled (p. 145)</a>	<p>The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.</p>
AC-2	ACCOUNT MANAGEMENT	<a href="#">iam-group-has-users-check (p. 153)</a>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AC-2	ACCOUNT MANAGEMENT	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC-2	ACCOUNT MANAGEMENT	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
AC-3	ACCESS ENFORCEMENT	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
AC-3	ACCESS ENFORCEMENT	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
AC-3	ACCESS ENFORCEMENT	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
AC-3	ACCESS ENFORCEMENT	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
AC-3	ACCESS ENFORCEMENT	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.

Control ID	Control Description	AWS Config Rule	Guidance
AC-3	ACCESS ENFORCEMENT	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC-3	ACCESS ENFORCEMENT	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
AC-3	ACCESS ENFORCEMENT	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC-3	ACCESS ENFORCEMENT	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
AC-3	ACCESS ENFORCEMENT	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
AC-17	REMOTE ACCESS	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
AC-17	REMOTE ACCESS	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
AC-17	REMOTE ACCESS	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
AC-17	REMOTE ACCESS	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
AC-17	REMOTE ACCESS	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
AC-17	REMOTE ACCESS	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
AU-2	AUDIT EVENTS	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.

Control ID	Control Description	AWS Config Rule	Guidance
AU-2	AUDIT EVENTS	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
AU-2	AUDIT EVENTS	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
AU-2	AUDIT EVENTS	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.

Control ID	Control Description	AWS Config Rule	Guidance
AU-9	PROTECTION OF AUDIT INFORMATION	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
AU-9	PROTECTION OF AUDIT INFORMATION	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
AU-9	PROTECTION OF AUDIT INFORMATION	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
AU-11	AUDIT RECORD RETENTION	<a href="#">cw-loggroup-retention-period-check (p. 125)</a>	Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. This rule allows you to optionally set the MinRetentionTime (FedRAMP Parameter: 90), as required by your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
CA-7	CONTINUOUS MONITORING	<a href="#">ec2-instance-detailed-monitoring-enabled (p. 132)</a>	Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance.
CA-7	CONTINUOUS MONITORING	<a href="#">rds-enhanced-monitoring-enabled (p. 165)</a>	Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics.

Control ID	Control Description	AWS Config Rule	Guidance
CM-2	BASELINE CONFIGURATION	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
CM-2	BASELINE CONFIGURATION	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
CM-2	BASELINE CONFIGURATION	<a href="#">ec2-stopped-instance (p. 137)</a>	Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards.

Control ID	Control Description	AWS Config Rule	Guidance
CM-2	BASELINE CONFIGURATION	<a href="#">ec2-volume-inuse-check (p. 137)</a>	This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality.
CM-2	BASELINE CONFIGURATION	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
CM-2	BASELINE CONFIGURATION	<a href="#">cloudtrail-security-trail-enabled (p. 118)</a>	This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions.

Control ID	Control Description	AWS Config Rule	Guidance
CM-8	INFORMATION SYSTEM COMPONENT INVENTORY	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
CP-9	INFORMATION SYSTEM BACKUP	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.
CP-9	INFORMATION SYSTEM BACKUP	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.

Control ID	Control Description	AWS Config Rule	Guidance
CP-9	INFORMATION SYSTEM BACKUP	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
CP-9	INFORMATION SYSTEM BACKUP	<a href="#">dynamodb-in-backup-plan (p. 128)</a>	To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
CP-9	INFORMATION SYSTEM BACKUP	<a href="#">ebs-in-backup-plan (p. 130)</a>	To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	Control Description	AWS Config Rule	Guidance
CP-9	INFORMATION SYSTEM BACKUP	<a href="#">efs-in-backup-plan (p. 139)</a>	To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
CP-9	INFORMATION SYSTEM BACKUP	<a href="#">rds-in-backup-plan (p. 167)</a>	To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	Control Description	AWS Config Rule	Guidance
CP-10	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	<a href="#">dynamodb-autoscaling-enabled (p. 128)</a>	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.
CP-10	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.

Control ID	Control Description	AWS Config Rule	Guidance
CP-10	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.
CP-10	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.

Control ID	Control Description	AWS Config Rule	Guidance
CP-10	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	<a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a>	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.
IA-2	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
IA-2	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
IA-2	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
IR-4	INCIDENT HANDLING	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (FedRAMP Parameter: 180), daysMediumSev (FedRAMP Parameter: 90), and daysHighSev (FedRAMP Parameter: 30) for non-archived findings, as required by your organization's policies.
SA-3	SYSTEM DEVELOPMENT LIFE CYCLE	<a href="#">codebuild-project-source-repo-url-check (p. 123)</a>	Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, user name and password within AWS Codebuild project environments. Use OAuth instead of personal access tokens or a user name and password to grant authorization for accessing GitHub or Bitbucket repositories.

Control ID	Control Description	AWS Config Rule	Guidance
SC-5	DENIAL OF SERVICE PROTECTION	<a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a>	The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.
SC-5	DENIAL OF SERVICE PROTECTION	<a href="#">rds-instance-deletion-protection-enabled (p. 166)</a>	Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
SC-7	BOUNDARY PROTECTION	<a href="#">alb-waf-enabled (p. 109)</a>	Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.

Control ID	Control Description	AWS Config Rule	Guidance
SC-7	BOUNDARY PROTECTION	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	<a href="#">cmk-backing-key-rotation-enabled (p. 123)</a>	Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period.
SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.
SC-13	CRYPTOGRAPHIC PROTECTION	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
SC-13	CRYPTOGRAPHIC PROTECTION	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.

Control ID	Control Description	AWS Config Rule	Guidance
SC-13	CRYPTOGRAPHIC PROTECTION	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
SC-13	CRYPTOGRAPHIC PROTECTION	<a href="#">dynamodb-table-encrypted-kms (p. 129)</a>	Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK).
SC-13	CRYPTOGRAPHIC PROTECTION	<a href="#">ec2-ebs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
SC-13	CRYPTOGRAPHIC PROTECTION	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
SC-13	CRYPTOGRAPHIC PROTECTION	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.

Control ID	Control Description	AWS Config Rule	Guidance
SC-13	CRYPTOGRAPHIC PROTECTION	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
SC-13	CRYPTOGRAPHIC PROTECTION	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.
SC-13	CRYPTOGRAPHIC PROTECTION	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SC-13	CRYPTOGRAPHIC PROTECTION	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
SC-13	CRYPTOGRAPHIC PROTECTION	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
SC-13	CRYPTOGRAPHIC PROTECTION	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SC-13	CRYPTOGRAPHIC PROTECTION	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.
SC-13	CRYPTOGRAPHIC PROTECTION	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.

## Template

The template is available on GitHub: [Operational Best Practices for FedRAMP\(Low\)](#).

## Operational Best Practices for FedRAMP(Moderate)

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Federal Risk and Authorization Management Program (FedRAMP) and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more FedRAMP controls. A FedRAMP control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This Conformance Pack was validated by AWS Security Assurance Services LLC (AWS SAS), which is a team of Payment Card Industry Qualified Security Assessors (QSAs), HITRUST Certified Common Security Framework Practitioners (CCSFPs), and compliance professionals certified to provide guidance and assessments for various industry frameworks. AWS SAS professionals designed this Conformance Pack to enable a customer to align to a subset of the FedRAMP controls.

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

Control ID	Control Description	AWS Config Rule	Guidance
AC-2(1)	The organization employs automated mechanisms to support the management of information system accounts.	<a href="#">secretsmanager-scheduled-rotation-success-check (p. 184)</a>	This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised.
AC-2(1)	The organization employs automated mechanisms to support the management of information system accounts.	<a href="#">iam-password-policy (p. 154)</a>	The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (FedRAMP Parameter: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password

Control ID	Control Description	AWS Config Rule	Guidance
			Policy. The actual values should reflect your organization's policies.
AC-2(1)	The organization employs automated mechanisms to support the management of information system accounts.	<a href="#">access-keys-rotated (p. 107)</a>	The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.
AC-2(1)	The organization employs automated mechanisms to support the management of information system accounts.	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AC-2(1)	The organization employs automated mechanisms to support the management of information system accounts.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC-2(1)	The organization employs automated mechanisms to support the management of information system accounts.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
AC-2(1)	The organization employs automated mechanisms to support the management of information system accounts.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
AC-2(3)	The information system automatically disables inactive accounts after 90 days for user accounts.	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (FedRAMP Parameter: 90). The actual value should reflect your organization's policies.
AC-2(4)	The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles].	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
AC-2(4)	The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles].	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
AC-2(4)	The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles].	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
AC-2(4)	The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles].	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	Control Description	AWS Config Rule	Guidance
AC-2(4)	The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles].	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
AC-2(4)	The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles].	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.

Control ID	Control Description	AWS Config Rule	Guidance
AC-2(4)	The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles].	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
AC-2(4)	The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles].	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AC-2(12)(a)	The organization: a. Monitors information system accounts for [Assignment: organization-defined atypical use].	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
AC-2(12)(a)	The organization: a. Monitors information system accounts for [Assignment: organization-defined atypical use].	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
AC-2(f)	The organization: f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions].	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AC-2(f)	The organization: f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions].	<a href="#">iam-password-policy (p. 154)</a>	The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (FedRAMP Parameter: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AC-2(f)	The organization: f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions].	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
AC-2(g)	The organization: g. Monitors the use of information system accounts.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AC-2(g)	The organization: g. Monitors the use of information system accounts.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
AC-2(g)	The organization: g. Monitors the use of information system accounts.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
AC-2(g)	The organization: g. Monitors the use of information system accounts.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.

Control ID	Control Description	AWS Config Rule	Guidance
AC-2(g)	The organization: g. Monitors the use of information system accounts.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
AC-2(g)	The organization: g. Monitors the use of information system accounts.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
AC-2(g)	The organization: g. Monitors the use of information system accounts.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.

Control ID	Control Description	AWS Config Rule	Guidance
AC-2(g)	The organization: g. Monitors the use of information system accounts.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
AC-2(j)	The organization: j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency].	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
AC-2(j)	The organization: j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency].	<a href="#">secretsmanager-scheduled-rotation-success-check (p. 184)</a>	This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised.
AC-2(j)	The organization: j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency].	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
AC-2(j)	<p>The organization: j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency].</p>	<p><a href="#">iam-password-policy (p. 154)</a></p>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (FedRAMP Parameter: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AC-2(j)	The organization: j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency].	<a href="#">access-keys-rotated (p. 107)</a>	The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.
AC-2(j)	The organization: j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency].	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.

Control ID	Control Description	AWS Config Rule	Guidance
AC-2(j)	The organization: j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency].	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
AC-2(j)	The organization: j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency].	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	Control Description	AWS Config Rule	Guidance
AC-2(j)	The organization: j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency].	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC-2(j)	The organization: j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency].	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.
AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.

Control ID	Control Description	AWS Config Rule	Guidance
AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	Control Description	AWS Config Rule	Guidance
AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC-3	The information system enforces approved authorizations for information access to information and system resources in accordance with applicable access control policies.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.

Control ID	Control Description	AWS Config Rule	Guidance
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.

Control ID	Control Description	AWS Config Rule	Guidance
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
AC-5c	The organization: c. Defines information system access authorizations to support separation of duties.	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.

Control ID	Control Description	AWS Config Rule	Guidance
AC-5c	The organization: c. Defines information system access authorizations to support separation of duties.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
AC-5c	The organization: c. Defines information system access authorizations to support separation of duties.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC-5c	The organization: c. Defines information system access authorizations to support separation of duties.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	Control Description	AWS Config Rule	Guidance
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">codebuild-project-envvar-awscred-check (p. 123)</a>	Ensure authentication credentials <code>AWS_ACCESS_KEY_ID</code> and <code>AWS_SECRET_ACCESS_KEY</code> do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access.
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	Control Description	AWS Config Rule	Guidance
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">ec2-imdsv2-check (p. 132)</a>	Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata.
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
AC-6(10)	The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.

Control ID	Control Description	AWS Config Rule	Guidance
AC-17(1)	The information system monitors and controls remote access methods.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
AC-17(1)	The information system monitors and controls remote access methods.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
AC-17(2)	The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
AC-17(2)	The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
AC-17(2)	The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.
AC-17(2)	The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
AC-17(2)	The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.

Control ID	Control Description	AWS Config Rule	Guidance
AC-17(2)	The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
AC-17(2)	The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
AC-17(3)	The information system routes all remote accesses through [Assignment: organization-defined number] managed network access control points.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
AC-21(b)	The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/ collaboration decisions.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
AC-21(b)	The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/ collaboration decisions.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
AC-21(b)	The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/ collaboration decisions.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
AC-21(b)	The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/ collaboration decisions.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
AC-21(b)	The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/ collaboration decisions.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
AC-21(b)	The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/ collaboration decisions.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
AC-21(b)	The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/ collaboration decisions.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
AC-21(b)	The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/ collaboration decisions.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
AC-21(b)	The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/ collaboration decisions.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC-21(b)	The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/ collaboration decisions.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
AC-21(b)	The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/ collaboration decisions.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC-21(b)	The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/ collaboration decisions.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
AU-2(a)(d)	<p>The organization:</p> <p>a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes. d. Determines that the following events are to be audited within the information system: [organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event].</p>	<p><a href="#">api-gw-execution-logging-enabled (p. 111)</a></p>	<p>API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AU-2(a)(d)	<p>The organization:</p> <p>a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes. d. Determines that the following events are to be audited within the information system: [organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event].</p>	<p><a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a></p>	<p>Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AU-2(a)(d)	<p>The organization:</p> <p>a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes. d. Determines that the following events are to be audited within the information system: [organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event].</p>	<p><a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a></p>	<p>The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AU-2(a)(d)	<p>The organization:</p> <p>a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes. d. Determines that the following events are to be audited within the information system: [organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event].</p>	<p><a href="#">cloudtrail-enabled (p. 121)</a></p>	<p>AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AU-2(a)(d)	<p>The organization:</p> <p>a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes. d. Determines that the following events are to be audited within the information system: [organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event].</p>	<p><a href="#">elb-logging-enabled (p. 144)</a></p>	<p>Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AU-2(a)(d)	<p>The organization:</p> <p>a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes. d. Determines that the following events are to be audited within the information system: [organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event].</p>	<p><a href="#">multi-region-cloudtrail-enabled (p. 163)</a></p>	<p>AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AU-2(a)(d)	<p>The organization:</p> <p>a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes. d. Determines that the following events are to be audited within the information system: [organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event].</p>	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	<p>Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AU-2(a)(d)	<p>The organization:</p> <p>a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes. d. Determines that the following events are to be audited within the information system: [organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event].</p>	<p><a href="#">vpc-flow-logs-enabled (p. 188)</a></p>	<p>The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AU-2(a)(d)	<p>The organization:</p> <p>a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes. d. Determines that the following events are to be audited within the information system: [organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event].</p>	<p><a href="#">rds-logging-enabled (p. 167)</a></p>	<p>To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AU-2(a)(d)	<p>The organization:</p> <p>a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes. d. Determines that the following events are to be audited within the information system: [organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event].</p>	<p><a href="#">wafv2-logging-enabled (p. 190)</a></p>	<p>To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AU-2(a)(d)	<p>The organization:</p> <p>a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes. d. Determines that the following events are to be audited within the information system: [organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event].</p>	<p><a href="#">redshift-cluster-configuration-check (p. 170)</a></p>	<p>To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.</p>
AU-3	<p>The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.</p>	<p><a href="#">api-gw-execution-logging-enabled (p. 111)</a></p>	<p>API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AU-3	The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
AU-3	The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
AU-3	The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.

Control ID	Control Description	AWS Config Rule	Guidance
AU-3	The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
AU-3	The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
AU-3	<p>The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.</p>	<p><a href="#">multi-region-cloudtrail-enabled (p. 163)</a></p>	<p>AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.</p>
AU-3	<p>The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.</p>	<p><a href="#">s3-bucket-logging-enabled (p. 177)</a></p>	<p>Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AU-3	The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
AU-3	The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AU-3	<p>The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.</p>	<p><a href="#">wafv2-logging-enabled (p. 190)</a></p>	<p>To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.</p>
AU-6(1)(3)	<p>(1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.</p>	<p><a href="#">cloudwatch-alarm-action-check (p. 119)</a></p>	<p>Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AU-6(1)(3)	(1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
AU-6(1)(3)	(1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
AU-6(1)(3)	(1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
AU-7(1)	The information system provides the capability to process audit records for events of interest based on [Assignment: organization-defined audit fields within audit records].	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), and <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
AU-7(1)	The information system provides the capability to process audit records for events of interest based on [Assignment: organization-defined audit fields within audit records].	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
AU-9	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
AU-9	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
AU-9(2)	The information system backs up audit records at least weekly onto a physically different system or system component than the system or component being audited.	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
AU-11	The organization retains audit records for at least 90 days to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	<a href="#">cw-loggroup-retention-period-check (p. 125)</a>	Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. This rule allows you to optionally set the MinRetentionTime (FedRAMP Parameter: 90), as required by your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AU-12(a)(c)	The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all information system and network components where audit capability is deployed/available c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
AU-12(a)(c)	The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all information system and network components where audit capability is deployed/available c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
AU-12(a)(c)	The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all information system and network components where audit capability is deployed/available c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.

Control ID	Control Description	AWS Config Rule	Guidance
AU-12(a)(c)	The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all information system and network components where audit capability is deployed/available c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
AU-12(a)(c)	The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all information system and network components where audit capability is deployed/available c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
AU-12(a)(c)	The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all information system and network components where audit capability is deployed/available c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
AU-12(a)(c)	<p>The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all information system and network components where audit capability is deployed/available c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.</p>	<p><a href="#">multi-region-cloudtrail-enabled (p. 163)</a></p>	<p>AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.</p>
AU-12(a)(c)	<p>The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all information system and network components where audit capability is deployed/available c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.</p>	<p><a href="#">s3-bucket-logging-enabled (p. 177)</a></p>	<p>Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AU-12(a)(c)	The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all information system and network components where audit capability is deployed/available c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
AU-12(a)(c)	The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all information system and network components where audit capability is deployed/available c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.

Control ID	Control Description	AWS Config Rule	Guidance
AU-12(a)(c)	<p>The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all information system and network components where audit capability is deployed/available c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.</p>	<p><a href="#">redshift-cluster-configuration-check (p. 170)</a></p>	<p>To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.</p>
CA-7(a)(b)	<p>The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring</p>	<p><a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a></p>	<p>Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.</p>

Control ID	Control Description	AWS Config Rule	Guidance
CA-7(a)(b)	<p>The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:</p> <ul style="list-style-type: none"> <li>a. Establishment of [Assignment: organization-defined metrics] to be monitored;</li> <li>b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring</li> </ul>	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	<p>Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), and <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.</p>
CA-7(a)(b)	<p>The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:</p> <ul style="list-style-type: none"> <li>a. Establishment of [Assignment: organization-defined metrics] to be monitored;</li> <li>b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring</li> </ul>	<a href="#">ec2-instance-detailed-monitoring-enabled (p. 132)</a>	<p>Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance.</p>

Control ID	Control Description	AWS Config Rule	Guidance
CA-7(a)(b)	The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring	<a href="#">rds-enhanced-monitoring-enabled (p. 165)</a>	Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics.
CA-7(a)(b)	The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
CA-7(a)(b)	<p>The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:</p> <ul style="list-style-type: none"> <li>a. Establishment of [Assignment: organization-defined metrics] to be monitored;</li> <li>b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring</li> </ul>	<a href="#">securityhub-enabled (p. 186)</a>	<p>AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.</p>
CM-2	<p>The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.</p>	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	<p>An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.</p>

Control ID	Control Description	AWS Config Rule	Guidance
CM-2	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
CM-2	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	<a href="#">ec2-stopped-instance (p. 137)</a>	Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards.
CM-2	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	<a href="#">ec2-volume-inuse-check (p. 137)</a>	This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality.

Control ID	Control Description	AWS Config Rule	Guidance
CM-2	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
CM-2	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
CM-2	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	<a href="#">cloudtrail-security-trail-enabled (p. 118)</a>	This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions.

Control ID	Control Description	AWS Config Rule	Guidance
CM-7(a)	The organization: a. Configures the information system to provide only essential capabilities.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
CM-7(a)	The organization: a. Configures the information system to provide only essential capabilities.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
CM-8(1)	The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
CM-8(3)(a)	The organization: a. Employs automated mechanisms continuously, using automated mechanisms with a maximum five-minute delay in detection, to detect the presence of unauthorized hardware, software, and firmware components within the information system	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
CM-8(3)(a)	The organization: a. Employs automated mechanisms continuously, using automated mechanisms with a maximum five-minute delay in detection, to detect the presence of unauthorized hardware, software, and firmware components within the information system	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
CM-8(3)(a)	The organization: a. Employs automated mechanisms continuously, using automated mechanisms with a maximum five-minute delay in detection, to detect the presence of unauthorized hardware, software, and firmware components within the information system	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
CP-9(b)	The organization: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full).	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.

Control ID	Control Description	AWS Config Rule	Guidance
CP-9(b)	The organization: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full).	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.
CP-9(b)	The organization: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full).	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
CP-9(b)	The organization: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full).	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.

Control ID	Control Description	AWS Config Rule	Guidance
CP-9(b)	The organization: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full).	<a href="#">dynamodb-in-backup-plan (p. 128)</a>	To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
CP-9(b)	The organization: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full).	<a href="#">ebs-in-backup-plan (p. 130)</a>	To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
CP-9(b)	The organization: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full).	<a href="#">efs-in-backup-plan (p. 139)</a>	To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	Control Description	AWS Config Rule	Guidance
CP-9(b)	The organization: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full).	<a href="#">rds-in-backup-plan (p. 167)</a>	To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	<a href="#">dynamodb-autoscaling-enabled (p. 128)</a>	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.

Control ID	Control Description	AWS Config Rule	Guidance
CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.

Control ID	Control Description	AWS Config Rule	Guidance
CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.
CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.
CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.

Control ID	Control Description	AWS Config Rule	Guidance
CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.

Control ID	Control Description	AWS Config Rule	Guidance
CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	<a href="#">dynamodb-in-backup-plan (p. 128)</a>	To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	<a href="#">ebs-in-backup-plan (p. 130)</a>	To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	<a href="#">efs-in-backup-plan (p. 139)</a>	To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	Control Description	AWS Config Rule	Guidance
CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	<a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a>	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.
CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	<a href="#">rds-in-backup-plan (p. 167)</a>	To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	Control Description	AWS Config Rule	Guidance
IA-2	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (FedRAMP Parameter: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
IA-2(1)	(1) The information system implements multifactor authentication for network access to privileged accounts.	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
IA-2(1)	(1) The information system implements multifactor authentication for network access to privileged accounts.	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
IA-2(1)(2)	(1) The information system implements multifactor authentication for network access to privileged accounts. (2) The information system implements multifactor authentication for network access to non-privileged accounts.	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
IA-2(1)(2)	(1) The information system implements multifactor authentication for network access to privileged accounts. (2) The information system implements multifactor authentication for network access to non-privileged accounts.	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.

Control ID	Control Description	AWS Config Rule	Guidance
IA-5(1)(a)(d)(e)	<p>The information system, for password-based authentication:</p> <p>a. Enforces minimum password complexity of [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type]; d. Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum]; e. Prohibits password reuse for 24 generations</p>	<p><a href="#">iam-password-policy (p. 154)</a></p>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (FedRAMP Parameter: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
IA-5(4)	The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy [Assignment: organization-defined requirements].	<a href="#">iam-password-policy (p. 154)</a>	The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (FedRAMP Parameter: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
IA-5(7)	The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.	<a href="#">codebuild-project-envvar-awscred-check (p. 123)</a>	Ensure authentication credentials <code>AWS_ACCESS_KEY_ID</code> and <code>AWS_SECRET_ACCESS_KEY</code> do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access.
IR-4(1)	The organization employs automated mechanisms to support the incident handling process.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.

Control ID	Control Description	AWS Config Rule	Guidance
IR-4(1)	The organization employs automated mechanisms to support the incident handling process.	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (FedRAMP Parameter: 180), daysMediumSev (FedRAMP Parameter: 90), and daysHighSev (FedRAMP Parameter: 30) for non-archived findings, as required by your organization's policies.
IR-6(1)	The organization employs automated mechanisms to assist in the reporting of security incidents.	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (FedRAMP Parameter: 180), daysMediumSev (FedRAMP Parameter: 90), and daysHighSev (FedRAMP Parameter: 30) for non-archived findings, as required by your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
IR-7(1)	The organization employs automated mechanisms to increase the availability of incident response-related information and support.	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (FedRAMP Parameter: 180), <code>daysMediumSev</code> (FedRAMP Parameter: 90), and <code>daysHighSev</code> (FedRAMP Parameter: 30) for non-archived findings, as required by your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
RA-5	<p>The organization: a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities [Assignment: organization-defined response times], in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate</p>	<p><a href="#">guardduty-enabled-centralized (p. 152)</a></p>	<p>Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).		

Control ID	Control Description	AWS Config Rule	Guidance
RA-5	<p>The organization: a. Scans for vulnerabilities in the information system and hosted applications monthly [operating system/ infrastructure; monthly web applications and databases] and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediate legitimate vulnerabilities: high-risk vulnerabilities mitigated within thirty (30) days from date of discovery; moderate-risk vulnerabilities mitigated within ninety (90) days from date of discovery; low risk vulnerabilities mitigated within one hundred and eighty (180) days from date of discovery, in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning</p>	<p><a href="#">guardduty-non-archived-findings (p. 152)</a></p>	<p>Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (FedRAMP Parameter: 180), daysMediumSev (FedRAMP Parameter: 90), and daysHighSev (FedRAMP Parameter: 30) for non-archived findings, as required by your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	<p>process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).</p>		
SA-3(a)	<p>The organization: a. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations.</p>	<p><a href="#">codebuild-project-envvar-awscred-check (p. 123)</a></p>	<p>Ensure authentication credentials <code>AWS_ACCESS_KEY_ID</code> and <code>AWS_SECRET_ACCESS_KEY</code> do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access.</p>
SA-3(a)	<p>The organization: a. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations.</p>	<p><a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a></p>	<p>An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SA-3(a)	The organization: a. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations.	<a href="#">codebuild-project-source-repo-url-check (p. 123)</a>	Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, user name and password within AWS Codebuild project environments. Use OAuth instead of personal access tokens or a user name and password to grant authorization for accessing GitHub or Bitbucket repositories.
SA-10	The organization requires the developer of the information system, system component, or information system service to: a. Perform configuration management during system, component, or service development, implementation, AND operation; b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management]; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
SA-10	The organization requires the developer of the information system, system component, or information system service to: a. Perform configuration management during system, component, or service development, implementation, AND operation; b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management]; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (FedRAMP Parameter: 180), daysMediumSev (FedRAMP Parameter: 90), and daysHighSev (FedRAMP Parameter: 30) for non-archived findings, as required by your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
SA-10	<p>The organization requires the developer of the information system, system component, or information system service to: a. Perform configuration management during system, component, or service development, implementation, AND operation; b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management]; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].</p>	<p><a href="#">securityhub-enabled (p. 186)</a></p>	<p>AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SA-10	The organization requires the developer of the information system, system component, or information system service to: a. Perform configuration management during system, component, or service development, implementation, AND operation; b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management]; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
SC-2	The information system separates user functionality (including user interface services) from information system management functionality.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
SC-2	The information system separates user functionality (including user interface services) from information system management functionality.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
SC-4	The information system prevents unauthorized and unintended information transfer via shared system resources.	<a href="#">ec2-volume-inuse-check (p. 137)</a>	This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality.
SC-5	The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards].	<a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a>	The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.
SC-5	The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards].	<a href="#">dynamodb-autoscaling-enabled (p. 128)</a>	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.

Control ID	Control Description	AWS Config Rule	Guidance
SC-5	The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards].	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
SC-5	The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards].	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.

Control ID	Control Description	AWS Config Rule	Guidance
SC-5	The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards].	<a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a>	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.
SC-5	The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards].	<a href="#">rds-instance-deletion-protection-enabled (p. 166)</a>	Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.

Control ID	Control Description	AWS Config Rule	Guidance
SC-7	The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.

Control ID	Control Description	AWS Config Rule	Guidance
SC-7	The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.

Control ID	Control Description	AWS Config Rule	Guidance
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">internet-gateway-authorized-vpc-only (p. 160)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.</p>
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">dms-replication-not-public (p. 127)</a></p>	<p>Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">ebs-snapshot-public-restorable-check (p. 131)</a></p>	<p>Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.</p>
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">ec2-instance-no-public-ip (p. 133)</a></p>	<p>Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">elasticsearch-in-vpc-only (p. 141)</a></p>	<p>Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.</p>
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">emr-master-no-public-ip (p. 146)</a></p>	<p>Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">restricted-ssh (p. 159)</a></p>	<p>Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.</p>
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">lambda-function-public-access-prohibited (p. 161)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">lambda-inside-vpc (p. 162)</a></p>	<p>Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.</p>
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">rds-instance-public-access-check (p. 166)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">rds-snapshots-public-prohibited (p. 168)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.</p>
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">redshift-cluster-public-access-check (p. 171)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">restricted-common-ports (p. 174)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.</p>
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">s3-account-level-public-access-blocks (p. 175)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">s3-bucket-public-read-prohibited (p. 179)</a></p>	<p>Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.</p>
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">s3-bucket-public-write-prohibited (p. 180)</a></p>	<p>Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.</p>
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">vpc-default-security-group-closed (p. 188)</a></p>	<p>Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">alb-http-to-https-redirect-check (p. 109)</a></p>	<p>To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.</p>
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">elb-tls-https-listeners-only (p. 145)</a></p>	<p>Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">s3-bucket-ssl-requests-only (p. 181)</a></p>	<p>To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.</p>
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">redshift-require-tls-ssl (p. 172)</a></p>	<p>Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">elb-acm-certificate-required (p. 143)</a></p>	<p>Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.</p>
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">alb-waf-enabled (p. 109)</a></p>	<p>Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">s3-bucket-policy-grantee-check (p. 178)</a></p>	<p>Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code>. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.</p>
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a></p>	<p>Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.</p>
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a></p>	<p>Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.

Control ID	Control Description	AWS Config Rule	Guidance
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.

Control ID	Control Description	AWS Config Rule	Guidance
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling s3_bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	Control Description	AWS Config Rule	Guidance
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
SC-8	The information system protects the confidentiality AND integrity of transmitted information.	<a href="#">alb-http-to-https-redirection-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC-8	The information system protects the confidentiality AND integrity of transmitted information.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC-8	The information system protects the confidentiality AND integrity of transmitted information.	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SC-8	The information system protects the confidentiality AND integrity of transmitted information.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC-8	The information system protects the confidentiality AND integrity of transmitted information.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC-8	The information system protects the confidentiality AND integrity of transmitted information.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
SC-8	The information system protects the confidentiality AND integrity of transmitted information.	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.

Control ID	Control Description	AWS Config Rule	Guidance
SC-8(1)	The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards].	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC-8(1)	The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards].	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC-8(1)	The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards].	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SC-8(1)	The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards].	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC-8(1)	The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards].	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC-8(1)	The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards].	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SC-8(1)	The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards].	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
SC-12	The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].	<a href="#">cmk-backing-key-rotation-enabled (p. 123)</a>	Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period.
SC-12	The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
SC-12	The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.
SC-13	The information system implements FIPS-validated or NSA-approved cryptography in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	<a href="#">dynamodb-table-encrypted-kms (p. 129)</a>	Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK).
SC-23	The information system protects the authenticity of communications sessions.	<a href="#">alb-http-to-https-redirection-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC-23	The information system protects the authenticity of communications sessions.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SC-23	The information system protects the authenticity of communications sessions.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC-28	The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest].	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
SC-28	The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest].	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
SC-28	The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest].	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
SC-28	The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest].	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
SC-28	The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest].	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.

Control ID	Control Description	AWS Config Rule	Guidance
SC-28	The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest].	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
SC-28	The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest].	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.
SC-28	The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest].	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
SC-28	The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest].	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.
SC-28	The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest].	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
SC-28	The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest].	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.
SC-28	The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest].	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SC-28	The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest].	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.
SC-28	The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest].	<a href="#">ec2-efs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
SC-28	The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest].	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.
SC-28	The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest].	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SI-2(2)	The organization employs automated mechanisms at least monthly to determine the state of information system components with regard to flaw remediation.	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
SI-2(2)	The organization employs automated mechanisms at least monthly to determine the state of information system components with regard to flaw remediation.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
SI-2(2)	The organization employs automated mechanisms at least monthly to determine the state of information system components with regard to flaw remediation.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
SI-4(1)	The organization connects and configures individual intrusion detection tools into an information system-wide intrusion detection system.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
SI-4(16)	The organization correlates information from monitoring tools employed throughout the information system.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
SI-4(16)	The organization correlates information from monitoring tools employed throughout the information system.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
SI-4(2)	The organization employs automated tools to support near real-time analysis of events.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
SI-4(2)	The organization employs automated tools to support near real-time analysis of events.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
SI-4(2)	The organization employs automated tools to support near real-time analysis of events.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
SI-4(2)	The organization employs automated tools to support near real-time analysis of events.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
SI-4(2)	The organization employs automated tools to support near real-time analysis of events.	<a href="#">ec2-instance-detailed-monitoring-enabled (p. 132)</a>	Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance.

Control ID	Control Description	AWS Config Rule	Guidance
SI-4(4)	The information system monitors inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
SI-4(4)	The information system monitors inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
SI-4(4)	The information system monitors inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), and <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
SI-4(4)	The information system monitors inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
SI-4(5)	The information system alerts [Assignment: organization-defined personnel or roles] when the following indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators].	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
SI-4(5)	The information system alerts [Assignment: organization-defined personnel or roles] when the following indications of compromise or potential compromise occur: [Assignment: organization- defined compromise indicators].	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
SI-4(5)	The information system alerts [Assignment: organization-defined personnel or roles] when the following indications of compromise or potential compromise occur: [Assignment: organization- defined compromise indicators].	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.

Control ID	Control Description	AWS Config Rule	Guidance
SI-4(5)	The information system alerts [Assignment: organization-defined personnel or roles] when the following indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators].	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
SI-4(a)(b)(c)	The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
SI-4(a)(b)(c)	<p>The organization:</p> <p>a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization- defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization- determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization.</p>	<p><a href="#">guardduty-non-archived-findings (p. 152)</a></p>	<p>Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (FedRAMP Parameter: 180), <code>daysMediumSev</code> (FedRAMP Parameter: 90), and <code>daysHighSev</code> (FedRAMP Parameter: 30) for non-archived findings, as required by your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SI-4(a)(b)(c)	<p>The organization:</p> <p>a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization- defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization- determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization.</p>	<p><a href="#">alb-waf-enabled (p. 109)</a></p>	<p>Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SI-4(a)(b)(c)	<p>The organization:</p> <p>a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization- defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization- determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization.</p>	<p><a href="#">wafv2-logging-enabled (p. 190)</a></p>	<p>To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SI-4(a)(b)(c)	<p>The organization:</p> <p>a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization- defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization- determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization.</p>	<p><a href="#">securityhub-enabled (p. 186)</a></p>	<p>AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SI-4(a)(b)(c)	<p>The organization:</p> <p>a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization- defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization- determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization.</p>	<p><a href="#">cloudwatch-alarm-action-check (p. 119)</a></p>	<p>Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), and <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SI-4(a)(b)(c)	The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization- defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization- determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
SI-4(a)(b)(c)	<p>The organization:</p> <p>a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization- defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization- determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization.</p>	<p><a href="#">ec2-instance-detailed-monitoring-enabled (p. 132)</a></p>	<p>Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance.</p>
SI-7	<p>The organization employs integrity verification tools to detect unauthorized changes to [Assignment: organization-defined software, firmware, and information].</p>	<p><a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a></p>	<p>Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SI-7(1)	The information system performs an integrity check security relevant events at least monthly.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
SI-7(1)	The information system performs an integrity check security relevant events at least monthly.	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.

Control ID	Control Description	AWS Config Rule	Guidance
SI-7(1)	The information system performs an integrity check security relevant events at least monthly.	<a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a>	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.
SI-12	The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.
SI-12	The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.

Control ID	Control Description	AWS Config Rule	Guidance
SI-12	The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.
SI-12	The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
SI-12	The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	<a href="#">rds-in-backup-plan (p. 167)</a>	To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	Control Description	AWS Config Rule	Guidance
SI-12	The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	<a href="#">ebs-in-backup-plan (p. 130)</a>	To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
SI-12	The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	<a href="#">efs-in-backup-plan (p. 139)</a>	To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
SI-12	The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	<a href="#">dynamodb-in-backup-plan (p. 128)</a>	To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	Control Description	AWS Config Rule	Guidance
SI-12	The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	<a href="#">cw-loggroup-retention-period-check (p. 125)</a>	Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. This rule allows you to optionally set the <code>MinRetentionTime</code> (FedRAMP Parameter: 90), as required by your organization's policies.

## Template

The template is available on GitHub: [Operational Best Practices for FedRAMP\(Moderate\)](#).

## Operational Best Practices for FFIEC

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Federal Financial Institutions Examination Council (FFIEC) Cyber Security Assessment Tool domains and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more FFIEC Cyber Security Assessment Tool controls. A FFIEC Cyber Security Assessment Tool control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This Conformance Pack was validated by AWS Security Assurance Services LLC (AWS SAS), which is a team of Payment Card Industry Qualified Security Assessors (QSAs), HITRUST Certified Common Security Framework Practitioners (CCSFPs), and compliance professionals certified to provide guidance and assessments for various industry frameworks. AWS SAS professionals designed this Conformance Pack to enable a customer to align to a subset of the FFIEC Cyber Security Assessment Tool.

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

Control ID	Control Description	AWS Config Rule	Guidance
D1.G.IT.B.1	An inventory of organizational assets (e.g., hardware, software, data, and systems hosted	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud

Control ID	Control Description	AWS Config Rule	Guidance
	externally) is maintained.		(Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
D1.G.RM.Rm.1	An information security and business continuity risk management function(s) exists within the institution.	<a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a>	The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.
D1.G.RM.Rm.1	An information security and business continuity risk management function(s) exists within the institution.	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.

Control ID	Control Description	AWS Config Rule	Guidance
D1.G.RM.Rm.1	An information security and business continuity risk management function(s) exists within the institution.	<a href="#">rds-in-backup-plan (p. 167)</a>	To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
D1.G.RM.Rm.1	An information security and business continuity risk management function(s) exists within the institution.	<a href="#">efs-in-backup-plan (p. 139)</a>	To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	Control Description	AWS Config Rule	Guidance
D1.G.RM.Rm.1	An information security and business continuity risk management function(s) exists within the institution.	<a href="#">ebs-in-backup-plan (p. 130)</a>	To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
D1.G.RM.Rm.1	An information security and business continuity risk management function(s) exists within the institution.	<a href="#">dynamodb-in-backup-plan (p. 128)</a>	To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
D1.G.RM.Rm.1	An information security and business continuity risk management function(s) exists within the institution.	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.

Control ID	Control Description	AWS Config Rule	Guidance
D1.G.RM.Rm.1	An information security and business continuity risk management function(s) exists within the institution.	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
D1.G.RM.Rm.1	An information security and business continuity risk management function(s) exists within the institution.	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.

Control ID	Control Description	AWS Config Rule	Guidance
D1.RM.RA.B.2	The risk assessment identifies Internet-based systems and high-risk transactions that warrant additional authentication controls.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
D2.TI.Ti.B.1	The institution belongs or subscribes to a threat and vulnerability information-sharing source(s) that provides information on threats (e.g., FS-ISAC, US-CERT).	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
D2.TI.Ti.B.2	Threat information is used to monitor threats and vulnerabilities.	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.

Control ID	Control Description	AWS Config Rule	Guidance
D2.MA.Ma.B.1	Audit log records and other security event logs are reviewed and retained in a secure manner.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
D2.MA.Ma.B.1	Audit log records and other security event logs are reviewed and retained in a secure manner.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
D2.MA.Ma.B.1	Audit log records and other security event logs are reviewed and retained in a secure manner.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
D2.MA.Ma.B.1	Audit log records and other security event logs are reviewed and retained in a secure manner.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
D2.MA.Ma.B.1	Audit log records and other security event logs are reviewed and retained in a secure manner.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
D2.MA.Ma.B.1	Audit log records and other security event logs are reviewed and retained in a secure manner.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
D2.MA.Ma.B.1	Audit log records and other security event logs are reviewed and retained in a secure manner.	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.
D2.MA.Ma.B.1	Audit log records and other security event logs are reviewed and retained in a secure manner.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
D2.MA.Ma.B.1	Audit log records and other security event logs are reviewed and retained in a secure manner.	<a href="#">cw-loggroup-retention-period-check (p. 125)</a>	Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events.

Control ID	Control Description	AWS Config Rule	Guidance
D2.MA.Ma.B.1	Audit log records and other security event logs are reviewed and retained in a secure manner.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
D2.MA.Ma.B.1	Audit log records and other security event logs are reviewed and retained in a secure manner.	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.

Control ID	Control Description	AWS Config Rule	Guidance
D2.MA.Ma.B.1	Audit log records and other security event logs are reviewed and retained in a secure manner.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
D2.MA.Ma.B.1	Audit log records and other security event logs are reviewed and retained in a secure manner.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
D2.IS.Is.B.1	Information security threats are gathered and shared with applicable internal employees.	<a href="#">cloudtrail-security-trail-enabled (p. 118)</a>	This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.Im.B.1	Network perimeter defense tools (e.g., border router and firewall) are used.	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.
D3.PC.Im.B.1	Network perimeter defense tools (e.g., border router and firewall) are used.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
D3.PC.Im.B.1	Network perimeter defense tools (e.g., border router and firewall) are used.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
D3.PC.Im.B.1	Network perimeter defense tools (e.g., border router and firewall) are used.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.Im.B.1	Network perimeter defense tools (e.g., border router and firewall) are used.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
D3.PC.Im.B.1	Network perimeter defense tools (e.g., border router and firewall) are used.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
D3.PC.Im.B.1	Network perimeter defense tools (e.g., border router and firewall) are used.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.Im.B.1	Network perimeter defense tools (e.g., border router and firewall) are used.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
D3.PC.Im.B.1	Network perimeter defense tools (e.g., border router and firewall) are used.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.Im.B.1	Network perimeter defense tools (e.g., border router and firewall) are used.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
D3.PC.Im.B.1	Network perimeter defense tools (e.g., border router and firewall) are used.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
D3.PC.Im.B.1	Network perimeter defense tools (e.g., border router and firewall) are used.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.Im.B.1	Network perimeter defense tools (e.g., border router and firewall) are used.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
D3.PC.Im.B.1	Network perimeter defense tools (e.g., border router and firewall) are used.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.Im.B.1	Network perimeter defense tools (e.g., border router and firewall) are used.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.
D3.PC.Im.B.1	Network perimeter defense tools (e.g., border router and firewall) are used.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
D3.PC.Im.B.1	Network perimeter defense tools (e.g., border router and firewall) are used.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.Im.B.1	Network perimeter defense tools (e.g., border router and firewall) are used.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
D3.PC.Im.B.1	Network perimeter defense tools (e.g., border router and firewall) are used.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
D3.PC.Im.B.1	Network perimeter defense tools (e.g., border router and firewall) are used.	<a href="#">alb-waf-enabled (p. 109)</a>	Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.Im.B.1	Network perimeter defense tools (e.g., border router and firewall) are used.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
D3.PC.Im.B.1	Network perimeter defense tools (e.g., border router and firewall) are used.	<a href="#">ec2-security-group-attached-to-eni (p. 137)</a>	This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment.
D3.PC.Im.B.1	Network perimeter defense tools (e.g., border router and firewall) are used.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.Am.B.1	Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
D3.PC.Im.B.7	Access to make changes to systems configurations (including virtual machines and hypervisors) is controlled and monitored.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
D3.PC.Im.B.7	Access to make changes to systems configurations (including virtual machines and hypervisors) is controlled and monitored.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.Im.B.7	Access to make changes to systems configurations (including virtual machines and hypervisors) is controlled and monitored.	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
D3.PC.Am.B.1	Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
D3.PC.Am.B.1	Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.Am.B.3	Elevated privileges (e.g., administrator privileges) are limited and tightly controlled (e.g., assigned to individuals, not shared, and require stronger password controls)	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
D3.PC.Am.B.3	Elevated privileges (e.g., administrator privileges) are limited and tightly controlled (e.g., assigned to individuals, not shared, and require stronger password controls)	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.Am.B.6	Identification and authentication are required and managed for access to systems, applications, and hardware.	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.Am.B.6	Identification and authentication are required and managed for access to systems, applications, and hardware.	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.Am.B.6	Identification and authentication are required and managed for access to systems, applications, and hardware.	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
D3.PC.Am.B.6	Identification and authentication are required and managed for access to systems, applications, and hardware.	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.Am.B.12	All passwords are encrypted in storage and in transit.	<a href="#">emr-kerberos-enabled (p. 145)</a>	<p>The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.</p>
D3.PC.Am.B.12	All passwords are encrypted in storage and in transit.	<a href="#">ec2-ebs-encryption-by-default (p. 131)</a>	<p>To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.Am.B.12	All passwords are encrypted in storage and in transit.	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
D3.PC.Am.B.12	All passwords are encrypted in storage and in transit.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
D3.PC.Am.B.12	All passwords are encrypted in storage and in transit.	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.
D3.PC.Am.B.12	All passwords are encrypted in storage and in transit.	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
D3.PC.Am.B.12	All passwords are encrypted in storage and in transit.	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.Am.B.12	All passwords are encrypted in storage and in transit.	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
D3.PC.Am.B.12	All passwords are encrypted in storage and in transit.	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
D3.PC.Am.B.12	All passwords are encrypted in storage and in transit.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
D3.PC.Am.B.12	All passwords are encrypted in storage and in transit.	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
D3.PC.Am.B.12	All passwords are encrypted in storage and in transit.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.Am.B.12	All passwords are encrypted in storage and in transit.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
D3.PC.Am.B.13	Confidential data is encrypted when transmitted across public or untrusted networks (e.g., Internet).	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
D3.PC.Im.B.5	Systems configurations (for servers, desktops, routers, etc.) follow industry standards and are enforced	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.Se.B.1	Developers working for the institution follow secure program coding practices, as part of a system development life cycle (SDLC), that meet industry standards.	<a href="#">codebuild-project-envvar-awscred-check (p. 123)</a>	Ensure authentication credentials <code>AWS_ACCESS_KEY_ID</code> and <code>AWS_SECRET_ACCESS_KEY</code> do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access.
D3.PC.Se.B.1	Developers working for the institution follow secure program coding practices, as part of a system development life cycle (SDLC), that meet industry standards.	<a href="#">codebuild-project-source-repo-url-check (p. 123)</a>	Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, user name and password within AWS Codebuild project environments. Use OAuth instead of personal access tokens or a user name and password to grant authorization for accessing GitHub or Bitbucket repositories.
D3.DC.An.B.1	The institution is able to detect anomalous activities through monitoring across the environment.	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
D3.DC.An.B.1	The institution is able to detect anomalous activities through monitoring across the environment.	<a href="#">ec2-instance-detailed-monitoring-enabled (p. 132)</a>	Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance.
D3.DC.An.B.1	The institution is able to detect anomalous activities through monitoring across the environment.	<a href="#">lambda-dlq-check (p. 161)</a>	Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed.
D3.DC.Ev.B.1	A normal network activity baseline is established.	<a href="#">lambda-concurrency-check (p. 161)</a>	This rule ensures that a Lambda function's concurrency high and low limits are established. This can assist in baselining the number of requests that your function is serving at any given time.
D5.IR.Pl.B.6	The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident.	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.

Control ID	Control Description	AWS Config Rule	Guidance
D5.IR.Pl.B.6	The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident.	<a href="#">dynamodb-autoscaling-enabled (p. 128)</a>	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.
D5.IR.Pl.B.6	The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident.	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.
D5.IR.Pl.B.6	The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident.	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.

Control ID	Control Description	AWS Config Rule	Guidance
D5.IR.PI.B.6	The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident.	<a href="#">dynamodb-throughput-limit-check (p. 130)</a>	Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set <code>accountRCUThresholdPercentage</code> (Config Default: 80) and <code>accountWCUThresholdPercentage</code> (Config Default: 80) parameters. The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
D5.IR.Pl.B.6	The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident.	<a href="#">rds-enhanced-monitoring-enabled (p. 165)</a>	Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics.
D5.IR.Pl.B.6	The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident.	<a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a>	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.

Control ID	Control Description	AWS Config Rule	Guidance
D5.IR.Pl.B.6	The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident.	<a href="#">rds-instance-deletion-protection-enabled (p. 166)</a>	Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
D5.IR.Pl.B.6	The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident.	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
D5.DR.De.B.1	Alert parameters are set for detecting information security incidents that prompt mitigating actions.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.

Control ID	Control Description	AWS Config Rule	Guidance
D2.TI.Ti.B.1	The institution belongs or subscribes to a threat and vulnerability information-sharing source(s) that provides information on threats (e.g., FS-ISAC, US-CERT).	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
D2.TI.Ti.B.2	Threat information is used to monitor threats and vulnerabilities.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
D2.TI.Ti.B.2	Threat information is used to monitor threats and vulnerabilities.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
D2.TI.Ti.B.3	Threat information is used to monitor threats and vulnerabilities.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
D2.TI.Ti.B.3	Threat information is used to monitor threats and vulnerabilities.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
D2.MA.Ma.B.2	Computer event logs are used for investigations once an event has occurred.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
D2.MA.Ma.B.2	Computer event logs are used for investigations once an event has occurred.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
D2.MA.Ma.B.2	Computer event logs are used for investigations once an event has occurred.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
D2.MA.Ma.B.2	Computer event logs are used for investigations once an event has occurred.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
D2.MA.Ma.B.2	Computer event logs are used for investigations once an event has occurred.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
D2.MA.Ma.B.2	Computer event logs are used for investigations once an event has occurred.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
D2.MA.Ma.B.2	Computer event logs are used for investigations once an event has occurred.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
D2.MA.Ma.B.2	Computer event logs are used for investigations once an event has occurred.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
D2.MA.Ma.B.2	Audit log records and other security event logs are reviewed and retained in a secure manner.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
D2.IS.Is.B.1	Information security threats are gathered and shared with applicable internal employees.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
D2.IS.Is.B.1	Information security threats are gathered and shared with applicable internal employees.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
D2.IS.Is.B.1	Information security threats are gathered and shared with applicable internal employees.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.IM.B.2	Systems that are accessed from the Internet or by external parties are protected by firewalls or other similar devices.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
D3.PC.IM.B.2	Systems that are accessed from the Internet or by external parties are protected by firewalls or other similar devices.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
D3.PC.IM.B.2	Systems that are accessed from the Internet or by external parties are protected by firewalls or other similar devices.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.IM.B.2	Systems that are accessed from the Internet or by external parties are protected by firewalls or other similar devices.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
D3.PC.IM.B.2	Systems that are accessed from the Internet or by external parties are protected by firewalls or other similar devices.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.IM.B.3	All ports are monitored.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
D3.PC.IM.B.3	All ports are monitored.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
D3.PC.IM.B.3	All ports are monitored.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
D3.PC.IM.B.3	All ports are monitored.	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.IM.B.3	All ports are monitored.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
D3.PC.IM.B.3	All ports are monitored.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
D3.PC.Im.B.5	Systems configurations (for servers, desktops, routers, etc.) follow industry standards and are enforced	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.Im.B.5	Systems configurations (for servers, desktops, routers, etc.) follow industry standards and are enforced	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
D3.PC.IM.B.6	Ports, functions, protocols and services are prohibited if no longer needed for business purposes.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
D3.PC.IM.B.6	Ports, functions, protocols and services are prohibited if no longer needed for business purposes.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.IM.B.6	Ports, functions, protocols and services are prohibited if no longer needed for business purposes.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
D3.PC.IM.B.6	Ports, functions, protocols and services are prohibited if no longer needed for business purposes.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.Im.B.7	Access to make changes to systems configurations (including virtual machines and hypervisors) is controlled and monitored.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
D3.PC.Im.B.7	Access to make changes to systems configurations (including virtual machines and hypervisors) is controlled and monitored.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
D3.PC.Im.B.7	Access to make changes to systems configurations (including virtual machines and hypervisors) is controlled and monitored.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.Am.B.1	Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
D3.PC.Am.B.1	Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
D3.PC.Am.B.1	Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege.	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.Am.B.2	Employee access to systems and confidential data provides for separation of duties.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
D3.PC.Am.B.2	Employee access to systems and confidential data provides for separation of duties.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
D3.PC.Am.B.3	Elevated privileges (e.g., administrator privileges) are limited and tightly controlled (e.g., assigned to individuals, not shared, and require stronger password controls).	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.Am.B.3	Elevated privileges (e.g., administrator privileges) are limited and tightly controlled (e.g., assigned to individuals, not shared, and require stronger password controls)	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
D3.PC.Am.B.3	Elevated privileges (e.g., administrator privileges) are limited and tightly controlled (e.g., assigned to individuals, not shared, and require stronger password controls)	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
D3.PC.Am.B.6	Identification and authentication are required and managed for access to systems, applications, and hardware.	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.Am.B.6	Identification and authentication are required and managed for access to systems, applications, and hardware.	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
D3.PC.Am.B.6	Identification and authentication are required and managed for access to systems, applications, and hardware.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
D3.PC.Am.B.6	Identification and authentication are required and managed for access to systems, applications, and hardware.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.Am.B.6	Identification and authentication are required and managed for access to systems, applications, and hardware.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
D3.PC.Am.B.6	Identification and authentication are required and managed for access to systems, applications, and hardware.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.Am.B.7	Access controls include password complexity and limits to password attempts and reuse.	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.Am.B.8	All default passwords and unnecessary default accounts are changed before system implementation.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
D3.PC.Am.B.10	Production and non-production environments are segregated to prevent unauthorized access or changes to information assets. (*N/A if no production environment exists at the institution or the institution's third party.)	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.Am.B.10	Production and non-production environments are segregated to prevent unauthorized access or changes to information assets. (*N/A if no production environment exists at the institution or the institution's third party.)	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
D3.PC.Am.B.10	Production and non-production environments are segregated to prevent unauthorized access or changes to information assets. (*N/A if no production environment exists at the institution or the institution's third party.)	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.Am.B.10	Production and non-production environments are segregated to prevent unauthorized access or changes to information assets. (*N/A if no production environment exists at the institution or the institution's third party.)	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
D3.PC.Am.B.12	All passwords are encrypted in storage and in transit.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.Am.B.13	Confidential data is encrypted when transmitted across public or untrusted networks (e.g., Internet).	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
D3.PC.Am.B.13	Confidential data is encrypted when transmitted across public or untrusted networks (e.g., Internet).	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
D3.PC.Am.B.13	Confidential data is encrypted when transmitted across public or untrusted networks (e.g., Internet).	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
D3.PC.Am.B.13	Confidential data is encrypted when transmitted across public or untrusted networks (e.g., Internet).	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
D3.PC.Am.B.13	Confidential data is encrypted when transmitted across public or untrusted networks (e.g., Internet).	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.Am.B.15	Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
D3.PC.Am.B.15	Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication.	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
D3.PC.Am.B.15	Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication.	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.Am.B.15	Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication.	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
D3.PC.Am.B.15	Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication.	<a href="#">alb-http-to-https-redirection-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
D3.PC.Am.B.15	Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
D3.PC.Am.B.15	Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication.	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.Am.B.15	Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
D3.PC.Am.B.16	Administrative, physical, or technical controls are in place to prevent users without administrative responsibilities from installing unauthorized software.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
D3.PC.Am.B.16	Administrative, physical, or technical controls are in place to prevent users without administrative responsibilities from installing unauthorized software.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	Control Description	AWS Config Rule	Guidance
D3.PC.Am.B.16	Administrative, physical, or technical controls are in place to prevent users without administrative responsibilities from installing unauthorized software.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
D3.DC.Th.B.1	Independent testing (including penetration testing and vulnerability scanning) is conducted according to the risk assessment for external-facing systems and the internal network.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
D3.DC.Th.B.1	Independent testing (including penetration testing and vulnerability scanning) is conducted according to the risk assessment for external-facing systems and the internal network.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
D3.DC.Th.B.1	Independent testing (including penetration testing and vulnerability scanning) is conducted according to the risk assessment for external-facing systems and the internal network.	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
D3.DC.An.B.1	The institution is able to detect anomalous activities through monitoring across the environment.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
D3.DC.An.B.1	The institution is able to detect anomalous activities through monitoring across the environment.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
D3.DC.An.B.2	Customer transactions generating anomalous activity alerts are monitored and reviewed.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
D3.DC.An.B.2	Customer transactions generating anomalous activity alerts are monitored and reviewed.	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
D3.DC.An.B.2	Customer transactions generating anomalous activity alerts are monitored and reviewed.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
D3.DC.An.B.3	Logs of physical and/or logical access are reviewed following events.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	Control Description	AWS Config Rule	Guidance
D3.DC.An.B.3	Logs of physical and/or logical access are reviewed following events.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
D3.DC.An.B.3	Logs of physical and/or logical access are reviewed following events.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
D3.DC.An.B.3	Logs of physical and/or logical access are reviewed following events.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
D3.DC.An.B.3	Logs of physical and/or logical access are reviewed following events.	<a href="#">cloudtrail-security-trail-enabled (p. 118)</a>	This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions.
D3.DC.An.B.3	Logs of physical and/or logical access are reviewed following events.	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.
D3.DC.An.B.3	Logs of physical and/or logical access are reviewed following events.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
D3.DC.An.B.3	Logs of physical and/or logical access are reviewed following events.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
D3.DC.An.B.3	Logs of physical and/or logical access are reviewed following events.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
D3.DC.An.B.3	Logs of physical and/or logical access are reviewed following events.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
D3.DC.An.B.3	Logs of physical and/or logical access are reviewed following events.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.

Control ID	Control Description	AWS Config Rule	Guidance
D3.DC.An.B.4	Access to critical systems by third parties is monitored for unauthorized or unusual activity	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
D3.DC.An.B.4	Access to critical systems by third parties is monitored for unauthorized or unusual activity	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.

Control ID	Control Description	AWS Config Rule	Guidance
D3.DC.An.B.4	Access to critical systems by third parties is monitored for unauthorized or unusual activity	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.
D3.DC.An.B.4	Access to critical systems by third parties is monitored for unauthorized or unusual activity	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
D3.DC.An.B.4	Access to critical systems by third parties is monitored for unauthorized or unusual activity	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.

Control ID	Control Description	AWS Config Rule	Guidance
D3.DC.An.B.4	Access to critical systems by third parties is monitored for unauthorized or unusual activity	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
D3.DC.An.B.4	Access to critical systems by third parties is monitored for unauthorized or unusual activity	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
D3.DC.An.B.4	Access to critical systems by third parties is monitored for unauthorized or unusual activity	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
D3.DC.An.B.4	Access to critical systems by third parties is monitored for unauthorized or unusual activity	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
D3.DC.An.B.4	Access to critical systems by third parties is monitored for unauthorized or unusual activity	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.

Control ID	Control Description	AWS Config Rule	Guidance
D3.DC.An.B.4	Access to critical systems by third parties is monitored for unauthorized or unusual activity	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
D3.DC.An.B.5	Elevated privileges are monitored.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
D3.DC.An.B.5	Elevated privileges are monitored.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
D3.DC.Ev.B.1	A normal network activity baseline is established.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.

Control ID	Control Description	AWS Config Rule	Guidance
D3.DC.Ev.B.1	A normal network activity baseline is established.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
D3.DC.Ev.B.1	A normal network activity baseline is established.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
D3.DC.Ev.B.1	A normal network activity baseline is established.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
D3.DC.Ev.B.1	A normal network activity baseline is established.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.

Control ID	Control Description	AWS Config Rule	Guidance
D3.DC.Ev.B.1	A normal network activity baseline is established.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
D3.DC.Ev.B.1	A normal network activity baseline is established.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
D3.DC.Ev.B.1	A normal network activity baseline is established.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
D3.DC.Ev.B.2	Mechanisms (e.g., antivirus alerts, log event alerts) are in place to alert management to potential attacks.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
D3.DC.Ev.B.3	Processes are in place to monitor for the presence of unauthorized users, devices, connections, and software.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.

Control ID	Control Description	AWS Config Rule	Guidance
D3.DC.Ev.B.3	Processes are in place to monitor for the presence of unauthorized users, devices, connections, and software.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
D3.DC.Ev.B.3	Processes are in place to monitor for the presence of unauthorized users, devices, connections, and software.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
D3.DC.Ev.B.3	Processes are in place to monitor for the presence of unauthorized users, devices, connections, and software.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	Control Description	AWS Config Rule	Guidance
D3.CC.PM.B.1	A patch management program is implemented and ensures that software and firmware patches are applied in a timely manner.	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
D3.CC.PM.B.3	Patch management reports are reviewed and reflect missing security patches.	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
D4.C.Co.B.2	The institution ensures that third-party connections are authorized.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.

Control ID	Control Description	AWS Config Rule	Guidance
D4.C.Co.B.2	The institution ensures that third-party connections are authorized.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
D4.C.Co.B.2	The institution ensures that third-party connections are authorized.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
D4.C.Co.B.2	The institution ensures that third-party connections are authorized.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
D5.IR.Pl.B.6	The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident.	<a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a>	The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.

Control ID	Control Description	AWS Config Rule	Guidance
D5.IR.Pl.B.6	The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident.	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
D5.IR.Pl.B.6	The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident.	<a href="#">rds-in-backup-plan (p. 167)</a>	To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
D5.IR.Pl.B.6	The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident.	<a href="#">efs-in-backup-plan (p. 139)</a>	To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	Control Description	AWS Config Rule	Guidance
D5.IR.Pl.B.6	The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident.	<a href="#">ebs-in-backup-plan (p. 130)</a>	To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
D5.IR.Pl.B.6	The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident.	<a href="#">dynamodb-in-backup-plan (p. 128)</a>	To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
D5.IR.Pl.B.6	The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident.	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.

Control ID	Control Description	AWS Config Rule	Guidance
D5.IR.Pl.B.6	The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident.	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
D5.IR.Pl.B.6	The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident.	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.

Control ID	Control Description	AWS Config Rule	Guidance
D5.IR.Pl.B.6	The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident.	<a href="#">lambda-concurrency-check (p. 161)</a>	This rule ensures that a Lambda function's concurrency high and low limits are established. This can assist in baselining the number of requests that your function is serving at any given time.
D5.DR.De.B.1	Alert parameters are set for detecting information security incidents that prompt mitigating actions.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
D5.DR.De.B.1	Alert parameters are set for detecting information security incidents that prompt mitigating actions.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
D5.DR.De.B.2	System performance reports contain information that can be used as a risk indicator to detect information security incidents	<a href="#">ec2-instance-detailed-monitoring-enabled (p. 132)</a>	Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance.
D5.DR.De.B.3	Tools and processes are in place to detect, alert, and trigger the incident response program.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
D5.DR.De.B.3	Tools and processes are in place to detect, alert, and trigger the incident response program.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
D5.DR.De.B.3	Tools and processes are in place to detect, alert, and trigger the incident response program.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
D5.DR.De.B.3	Tools and processes are in place to detect, alert, and trigger the incident response program.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.

Control ID	Control Description	AWS Config Rule	Guidance
D5.DR.De.B.3	Tools and processes are in place to detect, alert, and trigger the incident response program.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.
D5.DR.De.B.3	Tools and processes are in place to detect, alert, and trigger the incident response program.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
D5.DR.De.B.3	Tools and processes are in place to detect, alert, and trigger the incident response program.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
D5.DR.De.B.3	Tools and processes are in place to detect, alert, and trigger the incident response program.	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.
D5.DR.De.B.3	Tools and processes are in place to detect, alert, and trigger the incident response program.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
D5.DR.De.B.3	Tools and processes are in place to detect, alert, and trigger the incident response program.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
D5.DR.De.B.3	Tools and processes are in place to detect, alert, and trigger the incident response program.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
D5.DR.De.B.3	Tools and processes are in place to detect, alert, and trigger the incident response program.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
D5.ER.Es.B.4	Incidents are classified, logged and tracked.	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.

## Template

The template is available on GitHub: [Operational Best Practices for FFIEC](#).

## Operational Best Practices for HIPAA Security

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed

to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Health Insurance Portability and Accountability Act (HIPAA) and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more HIPAA controls. A HIPAA control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This Conformance Pack was validated by AWS Security Assurance Services LLC (AWS SAS), which is a team of Payment Card Industry Qualified Security Assessors (QSAs), HITRUST Certified Common Security Framework Practitioners (CCSFPs), and compliance professionals certified to provide guidance and assessments for various industry frameworks. AWS SAS professionals designed this Conformance Pack to enable a customer to align to a subset of the HIPAA.

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(1)(ii)(B)	Implement security measures to sufficiently reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">alb-http-to-https-redirection-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and	<a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a>	The Elastic Load Balancer (ELB) health checks for Amazon

Control ID	Control Description	AWS Config Rule	Guidance
	vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.		Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a>	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">codebuild-project-envvar-awscred-check (p. 123)</a>	Ensure authentication credentials <code>AWS_ACCESS_KEY_ID</code> and <code>AWS_SECRET_ACCESS_KEY</code> do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access.
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">codebuild-project-source-repo-url-check (p. 123)</a>	Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, user name and password within AWS Codebuild project environments. Use OAuth instead of personal access tokens or a user name and password to grant authorization for accessing GitHub or Bitbucket repositories.
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">dynamodb-autoscaling-enabled (p. 128)</a>	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">dynamodb-throughput-limit-check (p. 130)</a>	Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set <code>accountRCUThresholdPercentage</code> (Config Default: 80) and <code>accountWCUThresholdPercentage</code> (Config Default: 80) parameters. The actual values should reflect your organization's policies.
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">ec2-ebs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">ec2-stopped-instance (p. 137)</a>	Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
164.308(a)(1)(ii)(B)	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a): Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.
164.308(a)(1)(ii)(D)	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(1)(ii)(D)	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
164.308(a)(1)(ii)(D)	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
164.308(a)(1)(ii)(D)	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
164.308(a)(1)(ii)(D)	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(1)(ii)(D)	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
164.308(a)(1)(ii)(D)	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(1)(ii)(D)	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
164.308(a)(1)(ii)(D)	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(1)(ii)(D)	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
164.308(a)(1)(ii)(D)	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(3)(i)	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a) (4) of this section from obtaining access to electronic protected health information.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
164.308(a)(3)(i)	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a) (4) of this section from obtaining access to electronic protected health information.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(3)(i)	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a) (4) of this section from obtaining access to electronic protected health information.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
164.308(a)(3)(i)	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a) (4) of this section from obtaining access to electronic protected health information.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(3)(i)	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a) (4) of this section from obtaining access to electronic protected health information.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
164.308(a)(3)(i)	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a) (4) of this section from obtaining access to electronic protected health information.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(3)(i)	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a) (4) of this section from obtaining access to electronic protected health information.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
164.308(a)(3)(i)	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a) (4) of this section from obtaining access to electronic protected health information.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(3)(i)	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a) (4) of this section from obtaining access to electronic protected health information.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
164.308(a)(3)(i)	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a) (4) of this section from obtaining access to electronic protected health information.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(3)(i)	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a) (4) of this section from obtaining access to electronic protected health information.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
164.308(a)(3)(i)	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a) (4) of this section from obtaining access to electronic protected health information.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(3)(i)	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a) (4) of this section from obtaining access to electronic protected health information.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
164.308(a)(3)(i)	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a) (4) of this section from obtaining access to electronic protected health information.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(3)(i)	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a) (4) of this section from obtaining access to electronic protected health information.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
164.308(a)(3)(i)	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a) (4) of this section from obtaining access to electronic protected health information.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(3)(i)	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a) (4) of this section from obtaining access to electronic protected health information.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
164.308(a)(3)(i)	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a) (4) of this section from obtaining access to electronic protected health information.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(3)(i)	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a) (4) of this section from obtaining access to electronic protected health information.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
164.308(a)(3)(i)	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a) (4) of this section from obtaining access to electronic protected health information.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
164.308(a)(3)(ii)(a)	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(3)(ii)(A)	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
164.308(a)(3)(ii)(A)	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
164.308(a)(3)(ii)(A)	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(3)(ii)(A)	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
164.308(a)(3)(ii)(A)	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(3)(ii)(A)	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
164.308(a)(3)(ii)(A)	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(3)(ii)(A)	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
164.308(a)(3)(ii)(A)	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(3)(ii)(A)	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
164.308(a)(3)(ii)(A)	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(3)(ii)(A)	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
164.308(a)(3)(ii)(A)	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(3)(ii)(A)	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
164.308(a)(3)(ii)(B)	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
164.308(a)(3)(ii)(B)	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(3)(ii)(B)	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
164.308(a)(3)(ii)(B)	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
164.308(a)(3)(ii)(B)	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(3)(ii)(B)	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.
164.308(a)(3)(ii)(B)	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(3)(ii)(C)	Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(b).	<a href="#">access-keys-rotated (p. 107)</a>	The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.
164.308(a)(4)(i)	Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(4)(i)	Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
164.308(a)(4)(i)	Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
164.308(a)(4)(i)	Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(4)(ii)(B)	Implement policies and procedures for granting access to electronic protected health information, As one illustrative example, through access to a workstation, transaction, program, process, or other mechanism.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
164.308(a)(4)(ii)(B)	Implement policies and procedures for granting access to electronic protected health information, As one illustrative example, through access to a workstation, transaction, program, process, or other mechanism.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
164.308(a)(4)(ii)(B)	Implement policies and procedures for granting access to electronic protected health information, As one illustrative example, through access to a workstation, transaction, program, process, or other mechanism.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(4)(ii)(B)	Implement policies and procedures for granting access to electronic protected health information, As one illustrative example, through access to a workstation, transaction, program, process, or other mechanism.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
164.308(a)(4)(ii)(B)	Implement policies and procedures for granting access to electronic protected health information, As one illustrative example, through access to a workstation, transaction, program, process, or other mechanism.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
164.308(a)(4)(ii)(C)	Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	<a href="#">secretsmanager-rotation-enabled-check (p. 183)</a>	This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(4)(ii)(C)	Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	<a href="#">access-keys-rotated (p. 107)</a>	The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.
164.308(a)(4)(ii)(C)	Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(4)(ii)(C)	Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	<a href="#">iam-password-policy</a> (p. 154)	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(4)(ii)(C)	Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
164.308(a)(4)(ii)(C)	Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
164.308(a)(4)(ii)(C)	Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(4)(ii)(C)	Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
164.308(a)(4)(ii)(C)	Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.
164.308(a)(4)(ii)(C)	Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(6)(i)	Implement policies and procedures to address security incidents.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
164.308(a)(6)(i)	Implement policies and procedures to address security incidents.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
164.308(a)(6)(i)	Implement policies and procedures to address security incidents.	<a href="#">lambda-dlq-check (p. 161)</a>	Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(6)(i)	Implement policies and procedures to address security incidents.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
164.308(a)(6)(ii)	Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
164.308(a)(6)(ii)	Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(6)(ii)	Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
164.308(a)(6)(ii)	Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
164.308(a)(6)(ii)	Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(6)(ii)	Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
164.308(a)(6)(ii)	Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(6)(ii)	Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
164.308(a)(6)(ii)	Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(6)(ii)	Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
164.308(a)(6)(ii)	Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(7)(i)	Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.	<a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a>	The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.
164.308(a)(7)(i)	Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.	<a href="#">dynamodb-autoscaling-enabled (p. 128)</a>	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(7)(i)	Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
164.308(a)(7)(i)	Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(7)(i)	Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.
164.308(a)(7)(ii)(A)	Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.
164.308(a)(7)(ii)(A)	Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.

Control ID	Control Description	AWS Config Rule	Guidance
164.308(a)(7)(ii)(A)	Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
164.308(a)(7)(ii)(A)	Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.
164.308(a)(7)(ii)(A)	Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.

Control ID	Control Description	AWS Config Rule	Guidance
164.312(a)(1)	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4).	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
164.312(a)(1)	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4).	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
164.312(a)(1)	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4).	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
164.312(a)(1)	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4).	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
164.312(a)(1)	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4).	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.

Control ID	Control Description	AWS Config Rule	Guidance
164.312(a)(1)	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4).	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
164.312(a)(1)	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4).	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
164.312(a)(1)	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4).	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
164.312(a)(1)	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4).	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
164.312(a)(1)	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4).	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	Control Description	AWS Config Rule	Guidance
164.312(a)(1)	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4).	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
164.312(a)(1)	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4).	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
164.312(a)(1)	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4).	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
164.312(a)(1)	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4).	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
164.312(a)(1)	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4).	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
164.312(a)(1)	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4).	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
164.312(a)(1)	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4).	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
164.312(a)(1)	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4).	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.

Control ID	Control Description	AWS Config Rule	Guidance
164.312(a)(1)	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4).	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
164.312(a)(1)	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4).	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
164.312(a)(1)	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4).	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
164.312(a)(2)(i)	Assign a unique name and/or number for identifying and tracking user identity.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
164.312(a)(2)(ii)	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.
164.312(a)(2)(ii)	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.

Control ID	Control Description	AWS Config Rule	Guidance
164.312(a)(2)(ii)	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
164.312(a)(2)(ii)	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
164.312(a)(2)(ii)	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.

Control ID	Control Description	AWS Config Rule	Guidance
164.312(a)(2)(iv)	Implement a mechanism to encrypt and decrypt electronic protected health information.	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
164.312(a)(2)(iv)	Implement a mechanism to encrypt and decrypt electronic protected health information.	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
164.312(a)(2)(iv)	Implement a mechanism to encrypt and decrypt electronic protected health information.	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
164.312(a)(2)(iv)	Implement a mechanism to encrypt and decrypt electronic protected health information.	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
164.312(a)(2)(iv)	Implement a mechanism to encrypt and decrypt electronic protected health information.	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
164.312(a)(2)(iv)	Implement a mechanism to encrypt and decrypt electronic protected health information.	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.

Control ID	Control Description	AWS Config Rule	Guidance
164.312(a)(2)(iv)	Implement a mechanism to encrypt and decrypt electronic protected health information.	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.
164.312(a)(2)(iv)	Implement a mechanism to encrypt and decrypt electronic protected health information.	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.
164.312(a)(2)(iv)	Implement a mechanism to encrypt and decrypt electronic protected health information.	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
164.312(a)(2)(iv)	Implement a mechanism to encrypt and decrypt electronic protected health information.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
164.312(a)(2)(iv)	Implement a mechanism to encrypt and decrypt electronic protected health information.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
164.312(a)(2)(iv)	Implement a mechanism to encrypt and decrypt electronic protected health information.	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
164.312(a)(2)(iv)	Implement a mechanism to encrypt and decrypt electronic protected health information.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
164.312(a)(2)(iv)	Implement a mechanism to encrypt and decrypt electronic protected health information.	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.
164.312(a)(2)(iv)	Implement a mechanism to encrypt and decrypt electronic protected health information.	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.
164.312(a)(2)(iv)	Implement a mechanism to encrypt and decrypt electronic protected health information.	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
164.312(a)(2)(iv)	Implement a mechanism to encrypt and decrypt electronic protected health information.	<a href="#">ec2-ebs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
164.312(b)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
164.312(b)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
164.312(b)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	Control Description	AWS Config Rule	Guidance
164.312(b)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
164.312(b)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
164.312(b)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
164.312(b)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
164.312(b)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
164.312(b)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
164.312(b)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
164.312(b)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
164.312(c)(1)	Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	<a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a>	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.
164.312(c)(1)	Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
164.312(c)(1)	Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.
164.312(c)(2)	Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	<a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a>	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.
164.312(c)(2)	Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
164.312(c)(2)	Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.

Control ID	Control Description	AWS Config Rule	Guidance
164.312(d)	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
164.312(d)	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
164.312(d)	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
164.312(d)	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	Control Description	AWS Config Rule	Guidance
164.312(d)	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
164.312(e)(1)	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
164.312(e)(1)	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.

Control ID	Control Description	AWS Config Rule	Guidance
164.312(e)(1)	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
164.312(e)(1)	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.

Control ID	Control Description	AWS Config Rule	Guidance
164.312(e)(1)	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
164.312(e)(1)	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
164.312(e)(1)	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
164.312(e)(1)	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
164.312(e)(1)	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
164.312(e)(2)(i)	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
164.312(e)(2)(i)	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
164.312(e)(2)(i)	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
164.312(e)(2)(i)	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
164.312(e)(2)(i)	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.

Control ID	Control Description	AWS Config Rule	Guidance
164.312(e)(2)(i)	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
164.312(e)(2)(i)	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
164.312(e)(2)(i)	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
164.312(e)(2)(i)	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
164.312(e)(2)(i)	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
164.312(e)(2)(i)	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
164.312(e)(2)(ii)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	<a href="#">alb-http-to-https-redirection-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
164.312(e)(2)(ii)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
164.312(e)(2)(ii)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
164.312(e)(2)(ii)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
164.312(e)(2)(ii)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
164.312(e)(2)(ii)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.

Control ID	Control Description	AWS Config Rule	Guidance
164.312(e)(2)(ii)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
164.312(e)(2)(ii)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
164.312(e)(2)(ii)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.
164.312(e)(2)(ii)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
164.312(e)(2)(ii)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
164.312(e)(2)(ii)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
164.312(e)(2)(ii)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.
164.312(e)(2)(ii)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
164.312(e)(2)(ii)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.
164.312(e)(2)(ii)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	<a href="#">ec2-efs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
164.312(e)(2)(ii)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.

## Template

The template is available on GitHub: [Operational Best Practices for HIPAA Security](#).

## Operational Best Practices for K-ISMS

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between Korea – Information Security Management System (ISMS) and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to

one or more Korea – ISMS controls. A Korea – ISMS control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

Control ID	AWS Config Rule	Guidance
1.2.1	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
1.2.1	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
1.2.1	<a href="#">ec2-volume-inuse-check (p. 137)</a>	This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality.
1.2.1	<a href="#">eip-attached (p. 139)</a>	This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule

Control ID	AWS Config Rule	Guidance
		helps monitor unused EIPs in your environment.
2.1.3	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
2.1.3	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
2.1.3	<a href="#">ec2-volume-inuse-check (p. 137)</a>	This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality.
2.1.3	<a href="#">eip-attached (p. 139)</a>	This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment.

Control ID	AWS Config Rule	Guidance
2.3.3	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
2.3.3	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
2.5.1	<a href="#">access-keys-rotated (p. 107)</a>	The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
2.5.1	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
2.5.1	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
2.5.1	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.

Control ID	AWS Config Rule	Guidance
2.5.1	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
2.5.1	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
2.5.1	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
2.5.1	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
2.5.1	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
2.5.1	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
2.5.1	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
2.5.1	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.

Control ID	AWS Config Rule	Guidance
2.5.1	<a href="#">secretsmanager-rotation-enabled-check (p. 183)</a>	This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised.
2.5.1	<a href="#">secretsmanager-scheduled-rotation-success-check (p. 184)</a>	This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised.
2.5.1	<a href="#">iam-customer-policy-blocked-kms-actions (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the <code>blockedActionsPatterns</code> parameter. (AWS Foundational Security Best Practices value: <code>kms:Decrypt, kms:ReEncryptFrom</code> ). The actual values should reflect your organization's policie

Control ID	AWS Config Rule	Guidance
2.5.1	<a href="#">iam-inline-policy-blocked-kms-actions (p. 153)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the <code>blockedActionsPatterns</code> parameter. (AWS Foundational Security Best Practices value: <code>kms:Decrypt, kms:ReEncryptFrom</code> ). The actual values should reflect your organization's policies.
2.5.3	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
2.5.3	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.

Control ID	AWS Config Rule	Guidance
2.5.3	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
2.5.3	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	AWS Config Rule	Guidance
2.5.4	<a href="#">iam-password-policy (p. 154)</a>	The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.
2.5.5	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.

Control ID	AWS Config Rule	Guidance
2.5.5	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
2.5.5	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
2.5.5	<a href="#">secretsmanager-rotation-enabled-check (p. 183)</a>	This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised.
2.5.5	<a href="#">secretsmanager-scheduled-rotation-success-check (p. 184)</a>	This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised.
2.6	<a href="#">alb-waf-enabled (p. 109)</a>	Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.

Control ID	AWS Config Rule	Guidance
2.6	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
2.6	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
2.6	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
2.6	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
2.6	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
2.6	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
2.6	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
2.6	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
2.6	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.

Control ID	AWS Config Rule	Guidance
2.6	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
2.6	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
2.6	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
2.6	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
2.6	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
2.6	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
2.6	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
2.6	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	AWS Config Rule	Guidance
2.6	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
2.6	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.
2.6	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
2.6	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	AWS Config Rule	Guidance
2.6	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
2.6	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
2.6	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
2.6	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
2.6.4	<a href="#">secretsmanager-rotation-enabled-check (p. 183)</a>	This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised.

Control ID	AWS Config Rule	Guidance
2.6.4	<a href="#">secretsmanager-scheduled-rotation-success-check (p. 184)</a>	This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised.
2.6.6	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
2.6.6	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
2.6.6	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	AWS Config Rule	Guidance
2.6.6	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
2.6.6	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
2.6.6	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
2.6.6	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
2.6.6	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
2.6.6	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
2.6.6	<a href="#">ec2-imdsv2-check (p. 132)</a>	Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata.
2.6.6	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
2.7	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.
2.7	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
2.7	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	AWS Config Rule	Guidance
2.7	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
2.7	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
2.7	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
2.7	<a href="#">dynamodb-table-encrypted-kms (p. 129)</a>	Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK).
2.7	<a href="#">ec2-efs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
2.7	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
2.7	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.

Control ID	AWS Config Rule	Guidance
2.7	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
2.7	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
2.7	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
2.7	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
2.7	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.
2.7	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
2.7	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
2.7	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
2.7	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
2.7	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
2.7	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
2.7	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.
2.7	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.
2.7.2	<a href="#">cmk-backing-key-rotation-enabled (p. 123)</a>	Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period.
2.7.2	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.
2.8.5	<a href="#">codebuild-project-envvar-awscred-check (p. 123)</a>	Ensure authentication credentials <code>AWS_ACCESS_KEY_ID</code> and <code>AWS_SECRET_ACCESS_KEY</code> do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access.

Control ID	AWS Config Rule	Guidance
2.8.5	<a href="#">codebuild-project-source-repo-url-check (p. 123)</a>	Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, user name and password within AWS Codebuild project environments. Use OAuth instead of personal access tokens or a user name and password to grant authorization for accessing GitHub or Bitbucket repositories.
2.8.6	<a href="#">codebuild-project-envvar-awscred-check (p. 123)</a>	Ensure authentication credentials <code>AWS_ACCESS_KEY_ID</code> and <code>AWS_SECRET_ACCESS_KEY</code> do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access.
2.8.6	<a href="#">codebuild-project-source-repo-url-check (p. 123)</a>	Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, user name and password within AWS Codebuild project environments. Use OAuth instead of personal access tokens or a user name and password to grant authorization for accessing GitHub or Bitbucket repositories.
2.9.1	<a href="#">account-part-of-organizations (p. 108)</a>	Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data.

Control ID	AWS Config Rule	Guidance
2.9.1	<a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a>	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.
2.9.1	<a href="#">cloudtrail-security-trail-enabled (p. 118)</a>	This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions.
2.9.1	<a href="#">redshift-cluster-maintenancesettings-check (p. 171)</a>	This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferredMaintenanceWindow (the default is sat:16:00-sat:16:30), and the automatedSnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
2.9.2	<a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a>	The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.
2.9.2	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
2.9.2	<a href="#">dynamodb-throughput-limit-check (p. 130)</a>	Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set <code>accountRCUThresholdPercentage</code> (Config Default: 80) and <code>accountWCUThresholdPercentage</code> (Config Default: 80) parameters. The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
2.9.2	<a href="#">ec2-instance-detailed-monitoring-enabled (p. 132)</a>	Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance.
2.9.2	<a href="#">lambda-concurrency-check (p. 161)</a>	This rule ensures that a Lambda function's concurrency high and low limits are established. This can assist in baselining the number of requests that your function is serving at any given time.
2.9.2	<a href="#">lambda-dlq-check (p. 161)</a>	Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed.
2.9.2	<a href="#">rds-enhanced-monitoring-enabled (p. 165)</a>	Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics.
2.9.3	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.

Control ID	AWS Config Rule	Guidance
2.9.3	<a href="#">dynamodb-autoscaling-enabled (p. 128)</a>	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.
2.9.3	<a href="#">dynamodb-in-backup-plan (p. 128)</a>	To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
2.9.3	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.
2.9.3	<a href="#">ebs-in-backup-plan (p. 130)</a>	To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	AWS Config Rule	Guidance
2.9.3	<a href="#">ebs-optimized-instance (p. 131)</a>	An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance.
2.9.3	<a href="#">efs-in-backup-plan (p. 139)</a>	To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
2.9.3	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
2.9.3	<a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a>	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.

Control ID	AWS Config Rule	Guidance
2.9.3	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
2.9.3	<a href="#">rds-in-backup-plan (p. 167)</a>	To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
2.9.3	<a href="#">rds-instance-deletion-protection-enabled (p. 166)</a>	Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.

Control ID	AWS Config Rule	Guidance
2.9.3	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
2.9.3	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.
2.9.3	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
2.9.3	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.

Control ID	AWS Config Rule	Guidance
2.9.3	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.
2.9.4	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
2.9.4	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
2.9.4	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
2.9.4	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.

Control ID	AWS Config Rule	Guidance
2.9.4	<a href="#">cw-loggroup-retention-period-check (p. 125)</a>	Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events.
2.9.4	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
2.9.4	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
2.9.4	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.

Control ID	AWS Config Rule	Guidance
2.9.4	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
2.9.4	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
2.9.4	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.

Control ID	AWS Config Rule	Guidance
2.10.3	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
2.10.3	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
2.10.3	<a href="#">ec2-stopped-instance (p. 137)</a>	Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards.
2.10.3	<a href="#">ec2-volume-inuse-check (p. 137)</a>	This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality.

Control ID	AWS Config Rule	Guidance
2.10.3	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
2.10.3	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.
2.10.3	<a href="#">ec2-security-group-attached-to-eni (p. 137)</a>	This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment.
2.10.5	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
2.10.5	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	AWS Config Rule	Guidance
2.10.5	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
2.10.5	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
2.10.5	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
2.10.5	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
2.10.5	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	AWS Config Rule	Guidance
2.10.8	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
2.10.8	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
2.10.8	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.

Control ID	AWS Config Rule	Guidance
2.11.2	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.
2.11.3	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
2.11.3	<a href="#">ec2-instance-detailed-monitoring-enabled (p. 132)</a>	Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance.
2.11.3	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	AWS Config Rule	Guidance
2.11.3	<a href="#">lambda-concurrency-check (p. 161)</a>	This rule ensures that a Lambda function's concurrency high and low limits are established. This can assist in baselining the number of requests that your function is serving at any given time.
2.11.3	<a href="#">lambda-dlq-check (p. 161)</a>	Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed.
2.11.3	<a href="#">rds-enhanced-monitoring-enabled (p. 165)</a>	Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics.
2.11.3	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	AWS Config Rule	Guidance
2.12	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.
2.12	<a href="#">dynamodb-autoscaling-enabled (p. 128)</a>	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.
2.12	<a href="#">dynamodb-in-backup-plan (p. 128)</a>	To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
2.12	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.

Control ID	AWS Config Rule	Guidance
2.12	<a href="#">ebs-in-backup-plan (p. 130)</a>	To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
2.12	<a href="#">ebs-optimized-instance (p. 131)</a>	An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance.
2.12	<a href="#">efs-in-backup-plan (p. 139)</a>	To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
2.12	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.

Control ID	AWS Config Rule	Guidance
2.12	<a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a>	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.
2.12	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
2.12	<a href="#">rds-in-backup-plan (p. 167)</a>	To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
2.12	<a href="#">rds-instance-deletion-protection-enabled (p. 166)</a>	Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.

Control ID	AWS Config Rule	Guidance
2.12	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
2.12	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.
2.12	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
2.12	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.

Control ID	AWS Config Rule	Guidance
2.12	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.

## Template

The template is available on GitHub: [Operational Best Practices for K-ISMS](#).

## Operational Best Practices for Load Balancing

This pack contains AWS Config rules based on load balancing within AWS. This Conformance Pack has been designed for compatibility with the majority of AWS regions and to not require setting of any Parameters. Additional managed rules that require parameters to be set for your environment and/or for your specific region can be found at: [List of AWS Config Managed Rules](#).

See Parameters section for names and descriptions of required parameters.

The template is available on GitHub: [Operational Best Practices for Load Balancing](#).

## Operational Best Practices for Logging

This pack contains AWS Config rules based on logging within AWS. This Conformance Pack has been designed for compatibility with the majority of AWS regions and to not require setting of any Parameters. Additional managed rules that require parameters to be set for your environment and/or for your specific region can be found at: [List of AWS Config Managed Rules](#).

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

See Parameters section for names and descriptions of required parameters.

The template is available on GitHub: [Operational Best Practices for Logging](#).

## Operational Best Practices for Management and Governance Services

This pack contains AWS Config rules based on Management and Governance Services. For more information, see [Management and Governance on AWS](#). This Conformance Pack has been designed for compatibility with the majority of AWS regions and to not require setting of any Parameters. Additional

managed rules that require parameters to be set for your environment and/or for your specific region can be found at: [List of AWS Config Managed Rules](#).

See Parameters section for names and descriptions of required parameters.

The template is available on GitHub: [Operational Best Practices for Management and Governance Services](#).

## Operational Best Practices for MAS Notice 655

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Monetary Authority of Singapore (MAS) Notice 655 – Cyber Hygiene and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more MAS Notice 655 – Cyber Hygiene controls. A MAS Notice 655 – Cyber Hygiene control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

Control ID	AWS Config Rule	Guidance
4.1	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
4.1	<a href="#">access-keys-rotated (p. 107)</a>	The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.
4.1	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions

Control ID	AWS Config Rule	Guidance
		<p>and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.</p>
4.1	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	AWS Config Rule	Guidance
4.1	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
4.1	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
4.1	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
4.1	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.

Control ID	AWS Config Rule	Guidance
4.1	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
4.1	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
4.1	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	AWS Config Rule	Guidance
4.1	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
4.1	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
4.1	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
4.1	<a href="#">secretsmanager-rotation-enabled-check (p. 183)</a>	This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised.

Control ID	AWS Config Rule	Guidance
4.1	<a href="#">secretsmanager-scheduled-rotation-success-check (p. 184)</a>	This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised.
4.1	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
4.1	<a href="#">rds-instance-deletion-protection-enabled (p. 166)</a>	Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
4.2	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

Control ID	AWS Config Rule	Guidance
4.2	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
4.2	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
4.2	<a href="#">redshift-cluster-maintenancesettings-check (p. 171)</a>	This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the <code>allowVersionUpgrade</code> . The default is true. It also lets you optionally set the <code>preferredMaintenanceWindow</code> (the default is <code>sat:16:00-sat:16:30</code> ), and the <code>automatedSnapshotRetentionPeriod</code> (the default is 1). The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
4.2	<a href="#">ec2-imdsv2-check (p. 132)</a>	Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. With its new session-based controls, changes to instance metadata can be restricted. Additionally, updating to IMDSV2 can provide additional protection against misconfigured-open website application firewalls, reverse proxies, layer-3 firewalls and network address translation, as well as unpatched SSRF vulnerabilities.
4.3	<a href="#">codebuild-project-envvar-awscred-check (p. 123)</a>	Ensure authentication credentials <code>AWS_ACCESS_KEY_ID</code> and <code>AWS_SECRET_ACCESS_KEY</code> do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access.
4.4	<a href="#">alb-waf-enabled (p. 109)</a>	Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.
4.4	<a href="#">codebuild-project-envvar-awscred-check (p. 123)</a>	Ensure authentication credentials <code>AWS_ACCESS_KEY_ID</code> and <code>AWS_SECRET_ACCESS_KEY</code> do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access.

Control ID	AWS Config Rule	Guidance
4.4	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
4.4	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
4.4	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
4.4	<a href="#">ec2-security-group-attached-to-eni (p. 137)</a>	This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment.
4.4	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
4.4	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
4.4	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
4.4	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
4.4	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
4.4	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.

Control ID	AWS Config Rule	Guidance
4.4	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
4.4	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
4.4	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
4.4	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
4.4	<a href="#">redshift-cluster-public-access-check</a> (p. 171)	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
4.4	<a href="#">restricted-common-ports</a> (p. 174)	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
4.4	<a href="#">s3-account-level-public-access-blocks</a> (p. 175)	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
4.4	<a href="#">sagemaker-notebook-no-direct-internet-access</a> (p. 183)	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.

Control ID	AWS Config Rule	Guidance
4.4	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
4.4	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
4.5	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
4.5	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.

Control ID	AWS Config Rule	Guidance
4.5	<a href="#">ec2-managedinstance-association-compliance-status-check</a> (p. 135)	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
4.6	<a href="#">iam-password-policy</a> (p. 154)	The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
4.6	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
4.6	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
4.6	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
4.6	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.

Control ID	AWS Config Rule	Guidance
4.6	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
4.5	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

## Template

The template is available on GitHub: [Operational Best Practices for MAS Notice 655](#).

## Operational Best Practices for MAS TRMG June 2013

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Monetary Authority of Singapore (MAS) Technology Risk Management Guidelines (TRMG) June 2013 and AWS managed Config rules. Each AWS Config rule applies to a specific AWS resource, and relates to one or more Title 21 CFR Part 11 controls. A MAS TRMG June 2013 control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This Conformance Pack was validated by AWS Security Assurance Services LLC (AWS SAS), which is a team of Payment Card Industry Qualified Security Assessors (QSAs), HITRUST Certified Common Security Framework Practitioners (CCSFPs), and compliance professionals certified to provide guidance and assessments for various industry frameworks. AWS SAS professionals designed this Conformance Pack to enable you to align to a subset of MAS TRMG June 2013 design principles.

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

Control ID	AWS Config Rule	Guidance
4.1.1	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to

Control ID	AWS Config Rule	Guidance
		control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
4.1.1	<a href="#">ec2-imdsv2-check (p. 132)</a>	Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata.
4.1.1	<a href="#">secretsmanager-scheduled-rotation-success-check (p. 184)</a>	This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised.
4.1.1	<a href="#">secretsmanager-rotation-enabled-check (p. 183)</a>	This rule ensures AWS Secrets Manager secrets has rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active and reduce the business impact if the secret is compromised.
4.1.1	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or VPCs that you provide.

Control ID	AWS Config Rule	Guidance
4.1.1	<a href="#">access-keys-rotated (p. 107)</a>	The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.
4.1.1	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon EC2 instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
4.1.1	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
4.1.1	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.

Control ID	AWS Config Rule	Guidance
4.1.1	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.
4.1.1	<a href="#">rds-instance-deletion-protection-enabled (p. 166)</a>	Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
4.1.1	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
4.1.1	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	AWS Config Rule	Guidance
4.1.1	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>
4.1.1	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.</p>

Control ID	AWS Config Rule	Guidance
4.1.1	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
4.1.1	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
4.1.1	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
4.1.1	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	AWS Config Rule	Guidance
4.1.1	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.
4.1.1	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
4.1.1	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
4.1.1	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	AWS Config Rule	Guidance
4.1.1	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
4.1.1	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
4.1.1	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
4.1.1	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
4.1.1	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
4.1.1	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
4.1.1	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
4.1.1	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
4.1.1	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
4.1.1	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.
4.1.1	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
4.1.1	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.
4.1.1	<a href="#">ec2-ebs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
4.1.1	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.
4.1.1	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
4.1.1	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
4.1.1	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	AWS Config Rule	Guidance
4.1.1	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
4.1.1	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
4.1.1	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
4.1.1	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
4.2.1	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	AWS Config Rule	Guidance
4.2.1	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
4.2.1	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
4.2.1	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.
4.2.3	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	AWS Config Rule	Guidance
4.2.3	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
4.2.3	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
4.4.3	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.
4.5.1	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	AWS Config Rule	Guidance
4.5.1	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.
6.2.5	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
6.2.5	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	AWS Config Rule	Guidance
6.2.5	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
6.2.5	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
6.2.5	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
6.2.5	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	AWS Config Rule	Guidance
6.4.3	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
6.4.3	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
6.4.3	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
6.4.3	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	AWS Config Rule	Guidance
6.4.3	<a href="#">rds-instance-deletion-protection-enabled (p. 166)</a>	Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
6.4.3	<a href="#">rds-in-backup-plan (p. 167)</a>	To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
6.4.3	<a href="#">dynamodb-in-backup-plan (p. 128)</a>	To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
6.4.3	<a href="#">ebs-in-backup-plan (p. 130)</a>	To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	AWS Config Rule	Guidance
6.4.3	<a href="#">efs-in-backup-plan (p. 139)</a>	To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
6.4.3	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.
6.4.3	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
6.4.3	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.

Control ID	AWS Config Rule	Guidance
6.4.3	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
6.4.3	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
6.4.3	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.
6.4.3	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.
6.4.3	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	AWS Config Rule	Guidance
6.4.3	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
6.4.3	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
6.4.3	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
6.4.3	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
6.4.3	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
6.4.3	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
6.4.3	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.

Control ID	AWS Config Rule	Guidance
6.4.3	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.
6.4.3	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.
6.4.3	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
6.4.3	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
6.4.3	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
6.4.3	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
6.4.3	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.
6.4.3	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.
6.4.3	<a href="#">ec2-ebs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
6.4.3	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.
6.4.3	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
6.4.3	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	AWS Config Rule	Guidance
6.4.3	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
6.4.3	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
6.4.3	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
6.4.3	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
6.4.3	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
6.4.3	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.

Control ID	AWS Config Rule	Guidance
6.4.3	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
6.4.3	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
6.4.3	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
6.4.3	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	AWS Config Rule	Guidance
6.4.3	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
6.4.3	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
6.4.3	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
6.4.3	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
6.4.3	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.</p>
6.4.3	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	<p>Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.</p>
6.4.3	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.</p>
7.1.6	<a href="#">db-instance-backup-enabled (p. 126)</a>	<p>The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.</p>

Control ID	AWS Config Rule	Guidance
7.1.6	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.
7.1.6	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
7.1.6	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
7.1.6	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.

Control ID	AWS Config Rule	Guidance
7.1.6	<a href="#">dynamodb-in-backup-plan (p. 128)</a>	To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
7.1.6	<a href="#">ebs-in-backup-plan (p. 130)</a>	To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
7.1.6	<a href="#">efs-in-backup-plan (p. 139)</a>	To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
7.1.6	<a href="#">rds-in-backup-plan (p. 167)</a>	To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	AWS Config Rule	Guidance
7.1.7	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
7.1.7	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
7.1.7	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
7.1.7	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
7.1.7	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	AWS Config Rule	Guidance
7.1.7	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	<p>AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.</p>
7.1.7	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	<p>Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.</p>
7.1.7	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	<p>To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.</p>

Control ID	AWS Config Rule	Guidance
7.1.7	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
7.1.7	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
7.1.7	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.

Control ID	AWS Config Rule	Guidance
7.2.2	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
7.2.2	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
7.2.2	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
7.2.2	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
7.2.2	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
7.2.4	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
7.2.4	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	AWS Config Rule	Guidance
7.2.4	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
7.2.4	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
7.2.4	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
7.2.4	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.

Control ID	AWS Config Rule	Guidance
7.2.4	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
7.5.1	<a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a>	The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.
7.5.1	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
7.5.1	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.

Control ID	AWS Config Rule	Guidance
7.5.1	<a href="#">dynamodb-throughput-limit-check (p. 130)</a>	Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set <code>accountRCUThresholdPercentage</code> (Config Default: 80) and <code>accountWCUThresholdPercentage</code> (Config Default: 80) parameters. The actual values should reflect your organization's policies.
7.5.1	<a href="#">ec2-instance-detailed-monitoring-enabled (p. 132)</a>	Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance.
7.5.1	<a href="#">lambda-dlq-check (p. 161)</a>	Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed.
7.5.1	<a href="#">lambda-concurrency-check (p. 161)</a>	This rule ensures that a Lambda function's concurrency high and low limits are established. This can assist in baselining the number of requests that your function is serving at any given time.

Control ID	AWS Config Rule	Guidance
7.5.1	<a href="#">rds-enhanced-monitoring-enabled (p. 165)</a>	Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics.
7.5.2	<a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a>	The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.
7.5.2	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	AWS Config Rule	Guidance
7.5.2	<a href="#">dynamodb-throughput-limit-check (p. 130)</a>	Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set <code>accountRCUThresholdPercentage</code> (Config Default: 80) and <code>accountWCUThresholdPercentage</code> (Config Default: 80) parameters. The actual values should reflect your organization's policies.
7.5.2	<a href="#">ec2-instance-detailed-monitoring-enabled (p. 132)</a>	Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance.
7.5.2	<a href="#">lambda-concurrency-check (p. 161)</a>	This rule ensures that a Lambda function's concurrency high and low limits are established. This can assist in baselining the number of requests that your function is serving at any given time.
7.5.2	<a href="#">rds-enhanced-monitoring-enabled (p. 165)</a>	Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics.

Control ID	AWS Config Rule	Guidance
8.1.1	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.
8.1.1	<a href="#">dynamodb-autoscaling-enabled (p. 128)</a>	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.
8.1.1	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.
8.1.1	<a href="#">ebs-optimized-instance (p. 131)</a>	An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance.

Control ID	AWS Config Rule	Guidance
8.1.1	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
8.1.1	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
8.1.1	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
8.1.1	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
8.1.1	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
8.1.1	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.
8.1.1	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.
8.1.1	<a href="#">dynamodb-in-backup-plan (p. 128)</a>	To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	AWS Config Rule	Guidance
8.1.1	<a href="#">ebs-in-backup-plan (p. 130)</a>	To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
8.1.1	<a href="#">efs-in-backup-plan (p. 139)</a>	To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
8.1.1	<a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a>	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.
8.1.1	<a href="#">rds-instance-deletion-protection-enabled (p. 166)</a>	Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.

Control ID	AWS Config Rule	Guidance
8.1.1	<a href="#">rds-in-backup-plan (p. 167)</a>	To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
8.1.1	<a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a>	The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.
8.1.1	<a href="#">dynamodb-throughput-limit-check (p. 130)</a>	Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set <code>accountRCUThresholdPercentage</code> (Config Default: 80) and <code>accountWCUThresholdPercentage</code> (Config Default: 80) parameters. The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
8.1.1	<a href="#">ec2-instance-detailed-monitoring-enabled (p. 132)</a>	Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance.
8.1.1	<a href="#">lambda-concurrency-check (p. 161)</a>	This rule ensures that a Lambda function's concurrency high and low limits are established. This can assist in baselining the number of requests that your function is serving at any given time.
8.1.1	<a href="#">lambda-dlq-check (p. 161)</a>	Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed.
8.1.1	<a href="#">rds-enhanced-monitoring-enabled (p. 165)</a>	Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics.
8.1.2	<a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a>	The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.

Control ID	AWS Config Rule	Guidance
8.1.2	<a href="#">dynamodb-autoscaling-enabled (p. 128)</a>	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.
8.1.2	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
8.1.2	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.

Control ID	AWS Config Rule	Guidance
8.1.2	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.
8.1.2	<a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a>	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.
8.1.3	<a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a>	The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.

Control ID	AWS Config Rule	Guidance
8.1.3	<a href="#">dynamodb-throughput-limit-check (p. 130)</a>	Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set <code>accountRCUThresholdPercentage</code> (Config Default: 80) and <code>accountWCUThresholdPercentage</code> (Config Default: 80) parameters. The actual values should reflect your organization's policies.
8.1.3	<a href="#">dynamodb-autoscaling-enabled (p. 128)</a>	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.

Control ID	AWS Config Rule	Guidance
8.1.3	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
8.1.3	<a href="#">rds-instance-deletion-protection-enabled (p. 166)</a>	Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
8.1.3	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
8.1.3	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.

Control ID	AWS Config Rule	Guidance
8.1.3	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.
8.1.3	<a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a>	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.
8.4.1	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.
8.4.1	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.

Control ID	AWS Config Rule	Guidance
8.4.1	<a href="#">ebs-optimized-instance (p. 131)</a>	An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance.
8.4.1	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
8.4.1	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
8.4.1	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.

Control ID	AWS Config Rule	Guidance
8.4.1	<a href="#">dynamodb-in-backup-plan (p. 128)</a>	To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
8.4.1	<a href="#">ebs-in-backup-plan (p. 130)</a>	To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
8.4.1	<a href="#">efs-in-backup-plan (p. 139)</a>	To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
8.4.1	<a href="#">rds-in-backup-plan (p. 167)</a>	To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	AWS Config Rule	Guidance
9.0.1	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
9.1.6	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
9.1.6	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
9.1.6	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
9.1.6	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.

Control ID	AWS Config Rule	Guidance
9.1.6	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
9.1.6	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
9.1.6	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
9.1.6	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	AWS Config Rule	Guidance
9.1.6	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
9.1.6	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
9.1.6	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
9.1.6	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
9.1.6	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.
9.1.6	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
9.1.6	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
9.1.6	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.

Control ID	AWS Config Rule	Guidance
9.1.6	<a href="#">access-keys-rotated (p. 107)</a>	<p>The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.</p>
9.1.6	<a href="#">emr-kerberos-enabled (p. 145)</a>	<p>The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.</p>
9.1.6	<a href="#">iam-group-has-users-check (p. 153)</a>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.</p>

Control ID	AWS Config Rule	Guidance
9.1.6	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>
9.1.6	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.</p>

Control ID	AWS Config Rule	Guidance
9.1.6	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
9.1.6	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
9.1.6	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
9.1.6	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	AWS Config Rule	Guidance
9.1.6	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.
9.1.6	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
9.1.6	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
9.1.6	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	AWS Config Rule	Guidance
9.1.6	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
9.1.6	<a href="#">secretsmanager-rotation-enabled-check (p. 183)</a>	This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised.
9.1.6	<a href="#">secretsmanager-scheduled-rotation-success-check (p. 184)</a>	This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised.
9.1.6	<a href="#">ec2-imdsv2-check (p. 132)</a>	Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata.
9.1.6	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.

Control ID	AWS Config Rule	Guidance
9.1.6	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
9.1.6	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
9.1.6	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
9.1.6	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
9.1.6	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
9.1.6	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
9.1.6	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.

Control ID	AWS Config Rule	Guidance
9.1.6	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.
9.1.6	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
9.1.6	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
9.1.6	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
9.1.6	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.
9.1.6	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.
9.1.6	<a href="#">ec2-ebs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
9.1.6	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.
9.2.1	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

Control ID	AWS Config Rule	Guidance
9.2.1	<a href="#">ec2-security-group-attached-to-eni (p. 137)</a>	This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment.
9.2.1	<a href="#">eip-attached (p. 139)</a>	This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment.
9.2.1	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
9.2.2	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

Control ID	AWS Config Rule	Guidance
9.2.2	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
9.2.2	<a href="#">redshift-cluster-maintenancesettings-check (p. 171)</a>	This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferredMaintenanceWindow (the default is sat:16:00-sat:16:30), and the automatedSnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies.
9.3.1	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

Control ID	AWS Config Rule	Guidance
9.3.1	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
9.3.1	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
9.3.1	<a href="#">account-part-of-organizations (p. 108)</a>	Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data.

Control ID	AWS Config Rule	Guidance
9.3.1	<a href="#">emr-kerberos-enabled (p. 145)</a>	<p>The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.</p>
9.3.1	<a href="#">ec2-imdsv2-check (p. 132)</a>	<p>Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata.</p>

Control ID	AWS Config Rule	Guidance
9.3.1	<a href="#">iam-password-policy (p. 154)</a>	The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.
9.3.1	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.

Control ID	AWS Config Rule	Guidance
9.3.1	<a href="#">redshift-cluster-maintenancesettings-check (p. 171)</a>	<p>This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the <code>allowVersionUpgrade</code>. The default is <code>true</code>. It also lets you optionally set the <code>preferredMaintenanceWindow</code> (the default is <code>sat:16:00-sat:16:30</code>), and the <code>automatedSnapshotRetentionPeriod</code> (the default is <code>1</code>). The actual values should reflect your organization's policies.</p>
9.3.1	<a href="#">vpc-default-security-group-closed (p. 188)</a>	<p>Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.</p>
9.3.1	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	<p>Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.</p>
9.3.1	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	<p>Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.</p>

Control ID	AWS Config Rule	Guidance
9.3.1	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
9.3.1	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
9.3.1	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
9.3.1	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
9.3.1	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
9.3.1	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
9.3.1	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.
9.3.1	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
9.3.1	<a href="#">rds-instance-deletion-protection-enabled (p. 166)</a>	Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
9.3.1	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
9.3.1	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.
9.3.1	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	AWS Config Rule	Guidance
9.3.1	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
9.3.1	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
9.3.1	<a href="#">dynamodb-autoscaling-enabled (p. 128)</a>	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.
9.3.1	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	AWS Config Rule	Guidance
9.3.1	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
9.3.2	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment.
9.3.2	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	AWS Config Rule	Guidance
9.3.2	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
9.3.4	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
9.3.4	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
9.3.4	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	AWS Config Rule	Guidance
9.3.4	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
9.3.4	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
9.3.4	<a href="#">alb-waf-enabled (p. 109)</a>	Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.
9.5.1	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

Control ID	AWS Config Rule	Guidance
9.5.1	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
9.6.1	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
9.6.1	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
9.6.1	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	AWS Config Rule	Guidance
9.6.1	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
9.6.2	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
9.6.2	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
9.6.2	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	AWS Config Rule	Guidance
9.6.2	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
9.6.3	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
9.6.3	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
9.6.3	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.

Control ID	AWS Config Rule	Guidance
9.6.3	<a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a>	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.
9.6.3	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
9.6.4	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	AWS Config Rule	Guidance
9.6.4	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
9.6.4	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
9.6.4	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
9.6.6	<a href="#">cw-loggroup-retention-period-check (p. 125)</a>	Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events.
9.6.6	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.

Control ID	AWS Config Rule	Guidance
9.6.6	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
9.6.6	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.
9.6.6	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.
9.6.6	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
9.6.6	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.

Control ID	AWS Config Rule	Guidance
9.6.6	<a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a>	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.
11.0.1(b)	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
11.0.1(b)	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
11.0.1(b)	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	AWS Config Rule	Guidance
11.0.1(b)	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
11.0.1(b)	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
11.0.1(b)	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
11.0.1(c)	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	AWS Config Rule	Guidance
11.0.1(c)	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
11.0.1(c)	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
11.0.1(c)	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
11.0.1(c)	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.

Control ID	AWS Config Rule	Guidance
11.0.1(c)	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
11.0.1(c)	<a href="#">ec2-imdsv2-check (p. 132)</a>	Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata.
11.0.1(c)	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
11.1.2	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	AWS Config Rule	Guidance
11.1.2	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
11.1.2	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
11.1.2	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
11.1.2	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.

Control ID	AWS Config Rule	Guidance
11.1.2	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
11.1.2	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
11.1.2	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
11.1.2	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	AWS Config Rule	Guidance
11.1.2	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
11.1.2	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
11.1.2	<a href="#">ec2-imdsv2-check (p. 132)</a>	Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata.
11.1.2	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.

Control ID	AWS Config Rule	Guidance
11.1.3	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
11.1.3	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
11.1.3	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
11.1.3	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
11.1.3	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.

Control ID	AWS Config Rule	Guidance
11.1.3	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
11.1.5	<a href="#">iam-password-policy (p. 154)</a>	The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.
11.1.6	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	AWS Config Rule	Guidance
11.1.6	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
11.1.6	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
11.1.6	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
11.1.6	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	AWS Config Rule	Guidance
11.2.3(a)	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
11.2.3(a)	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
11.2.3(a)	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
11.2.3(a)	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	AWS Config Rule	Guidance
11.2.3(b)	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
11.2.3(b)	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
11.2.3(b)	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
11.2.3(b)	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.

Control ID	AWS Config Rule	Guidance
11.2.3(c)	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
11.2.3(c)	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
11.2.3(c)	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
11.2.3(c)	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.

Control ID	AWS Config Rule	Guidance
11.2.3(c)	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
11.2.3(c)	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
11.2.3(d)	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
11.2.3(d)	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	AWS Config Rule	Guidance
11.2.3(d)	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
11.2.3(d)	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
11.2.3(d)	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
11.2.3(d)	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.

Control ID	AWS Config Rule	Guidance
11.2.3(e)	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
11.2.3(e)	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
11.2.3(e)	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
11.2.3(e)	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
11.2.3(e)	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.

Control ID	AWS Config Rule	Guidance
11.2.3(e)	<a href="#">cw-loggroup-retention-period-check (p. 125)</a>	Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events.
11.2.3(e)	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
11.2.3(e)	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	AWS Config Rule	Guidance
11.2.3(e)	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
11.2.3(e)	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
11.2.3(f)	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
11.2.3(f)	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	AWS Config Rule	Guidance
11.2.3(f)	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
11.2.3(f)	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
11.2.3(f)	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
11.2.3(f)	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling s3_bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.

Control ID	AWS Config Rule	Guidance
11.2.3(h)	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
11.2.3(j)	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
11.2.3(j)	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
11.2.3(j)	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	AWS Config Rule	Guidance
11.2.3(j)	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
11.2.3(j)	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
11.2.3(j)	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling s3_bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
12.1.1	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	AWS Config Rule	Guidance
12.1.1	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
12.1.1	<a href="#">cloudtrail-security-trail-enabled (p. 118)</a>	This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions.
12.1.1	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
12.1.1	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

Control ID	AWS Config Rule	Guidance
12.1.1	<a href="#">ec2-stopped-instance (p. 137)</a>	Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards.
12.1.1	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
12.1.1	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
12.1.1	<a href="#">ec2-volume-inuse-check (p. 137)</a>	This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality.

Control ID	AWS Config Rule	Guidance
12.1.1	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.
12.1.1	<a href="#">dynamodb-autoscaling-enabled (p. 128)</a>	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.
12.1.1	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.
12.1.1	<a href="#">ebs-optimized-instance (p. 131)</a>	An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance.

Control ID	AWS Config Rule	Guidance
12.1.1	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
12.1.1	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
12.1.1	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
12.1.1	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
12.1.1	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
12.1.1	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.
12.1.1	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.
12.1.1	<a href="#">dynamodb-in-backup-plan (p. 128)</a>	To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	AWS Config Rule	Guidance
12.1.1	<a href="#">ebs-in-backup-plan (p. 130)</a>	To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
12.1.1	<a href="#">efs-in-backup-plan (p. 139)</a>	To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
12.1.1	<a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a>	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.
12.1.1	<a href="#">rds-instance-deletion-protection-enabled (p. 166)</a>	Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.

Control ID	AWS Config Rule	Guidance
12.1.1	<a href="#">rds-in-backup-plan (p. 167)</a>	To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
12.1.1	<a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a>	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.
12.1.1	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.
12.1.1	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	AWS Config Rule	Guidance
12.1.1	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
12.1.1	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
12.1.1	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
12.1.1	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
12.1.1	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
12.1.1	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
12.1.1	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.

Control ID	AWS Config Rule	Guidance
12.1.1	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.
12.1.1	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.
12.1.1	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
12.1.1	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	AWS Config Rule	Guidance
12.1.1	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
12.1.1	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
12.1.1	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.
12.1.1	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.
12.1.1	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.
12.1.1	<a href="#">ec2-efs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
12.1.1	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.
12.1.1	<a href="#">cmk-backing-key-rotation-enabled (p. 123)</a>	Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period.
12.1.1	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
12.1.1	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
12.1.1	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
12.1.1	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
12.1.1	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.

Control ID	AWS Config Rule	Guidance
12.1.1	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
12.1.1	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
12.1.1	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	AWS Config Rule	Guidance
12.1.1	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
12.1.1	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
12.1.1	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.
12.1.1	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
12.1.1	<a href="#">lambda-dlq-check (p. 161)</a>	Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed.

Control ID	AWS Config Rule	Guidance
12.1.1	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
12.1.1	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
12.1.1	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
12.1.1	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.

Control ID	AWS Config Rule	Guidance
12.1.1	<a href="#">alb-waf-enabled (p. 109)</a>	Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.
12.1.1	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
12.1.1	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
12.1.1	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
12.1.1	<a href="#">codebuild-project-envvar-awscred-check (p. 123)</a>	Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access.

Control ID	AWS Config Rule	Guidance
12.1.1	<a href="#">codebuild-project-source-repo-url-check (p. 123)</a>	Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, user name and password within AWS Codebuild project environments. Use OAuth instead of personal access tokens or a user name and password to grant authorization for accessing GitHub or Bitbucket repositories.
12.1.1	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.
12.1.4	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
12.1.4	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	AWS Config Rule	Guidance
12.1.4	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
12.1.4	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
12.1.4	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	AWS Config Rule	Guidance
12.1.4	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>
12.1.4	<a href="#">iam-no-inline-policy-check (p. 154)</a>	<p>Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.</p>

Control ID	AWS Config Rule	Guidance
12.1.4	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
12.1.4	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
12.1.4	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
12.1.4	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	AWS Config Rule	Guidance
12.1.4	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
12.1.4	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
12.1.4	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
12.1.4	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
12.1.4	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
12.1.4	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
12.1.4	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
12.1.4	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
12.1.4	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.

Control ID	AWS Config Rule	Guidance
12.1.4	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
12.1.4	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
12.1.4	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
12.1.4	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
12.1.4	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
12.1.4	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.
12.1.4	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
12.1.4	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
12.1.4	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.

Control ID	AWS Config Rule	Guidance
12.1.4	<a href="#">alb-waf-enabled (p. 109)</a>	Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.
12.1.4	<a href="#">ec2-imdsv2-check (p. 132)</a>	Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata.
12.1.4	<a href="#">alb-http-to-https-redirection-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
12.1.4	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
12.1.4	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	AWS Config Rule	Guidance
12.1.4	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
12.1.4	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
12.1.4	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
12.1.4	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
12.1.4	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.

Control ID	AWS Config Rule	Guidance
12.1.4	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
12.1.5	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
12.1.5	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
12.1.5	<a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a>	The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.

Control ID	AWS Config Rule	Guidance
12.1.5	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
12.1.5	<a href="#">lambda-dlq-check (p. 161)</a>	Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed.
12.1.5	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
12.1.5	<a href="#">ec2-instance-detailed-monitoring-enabled (p. 132)</a>	Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance.

Control ID	AWS Config Rule	Guidance
12.1.5	<a href="#">rds-enhanced-monitoring-enabled (p. 165)</a>	Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics.
12.1.6	<a href="#">dynamodb-autoscaling-enabled (p. 128)</a>	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.
12.1.6	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.

Control ID	AWS Config Rule	Guidance
12.1.6	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
12.1.6	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.
12.1.6	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.

Control ID	AWS Config Rule	Guidance
12.1.6	<a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a>	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.
12.1.6	<a href="#">rds-instance-deletion-protection-enabled (p. 166)</a>	Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
12.2.4	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.
12.2.4	<a href="#">alb-http-to-https-redirection-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
12.2.4	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
12.2.4	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
12.2.4	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
12.2.4	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
12.2.4	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
12.2.4	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
12.2.4	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
12.2.4	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.

Control ID	AWS Config Rule	Guidance
12.2.4	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.
12.2.4	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
12.2.4	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
12.2.4	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
12.2.4	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	AWS Config Rule	Guidance
12.2.4	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.
12.2.4	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.
12.2.4	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.
12.2.4	<a href="#">ec2-efs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
12.2.4	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.
12.2.4	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	AWS Config Rule	Guidance
12.2.4	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
12.2.4	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
A.1.2	<a href="#">codebuild-project-envvar-awscred-check (p. 123)</a>	Ensure authentication credentials <code>AWS_ACCESS_KEY_ID</code> and <code>AWS_SECRET_ACCESS_KEY</code> do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access.
A.1.2	<a href="#">codebuild-project-source-repo-url-check (p. 123)</a>	Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, user name and password within AWS Codebuild project environments. Use OAuth instead of personal access tokens or a user name and password to grant authorization for accessing GitHub or Bitbucket repositories.

Control ID	AWS Config Rule	Guidance
B.2.4	<a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a>	The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.
B.2.4	<a href="#">dynamodb-throughput-limit-check (p. 130)</a>	Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set <code>accountRCUThresholdPercentage</code> (Config Default: 80) and <code>accountWCUThresholdPercentage</code> (Config Default: 80) parameters. The actual values should reflect your organization's policies.
B.2.4	<a href="#">rds-enhanced-monitoring-enabled (p. 165)</a>	Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics.

Control ID	AWS Config Rule	Guidance
B.2.4	<a href="#">ec2-instance-detailed-monitoring-enabled (p. 132)</a>	Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance.
B.2.4	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
B.2.4	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
B.3.1	<a href="#">dynamodb-autoscaling-enabled (p. 128)</a>	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.

Control ID	AWS Config Rule	Guidance
B.3.1	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
B.3.1	<a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a>	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.
C.3.1	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
C.3.1	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.
C.3.1	<a href="#">cmk-backing-key-rotation-enabled (p. 123)</a>	Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period.
D.2.2	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
D.2.2	<a href="#">alb-waf-enabled (p. 109)</a>	Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.
D.2.3	<a href="#">ebs-optimized-instance (p. 131)</a>	An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance.

Control ID	AWS Config Rule	Guidance
D.2.3	<a href="#">dynamodb-autoscaling-enabled (p. 128)</a>	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.
D.2.3	<a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a>	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.
D.2.3	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.

Control ID	AWS Config Rule	Guidance
D.2.3	<a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a>	The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.
D.2.3	<a href="#">dynamodb-throughput-limit-check (p. 130)</a>	Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set <code>accountRCUThresholdPercentage</code> (Config Default: 80) and <code>accountWCUThresholdPercentage</code> (Config Default: 80) parameters. The actual values should reflect your organization's policies.
D.2.3	<a href="#">lambda-concurrency-check (p. 161)</a>	This rule ensures that a Lambda function's concurrency high and low limits are established. This can assist in baselining the number of requests that your function is serving at any given time.
E.2.5	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	AWS Config Rule	Guidance
E.2.5	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
E.2.5	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
E.2.5	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
E.2.5	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
E.2.5	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
E.2.5	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.

## Template

The template is available on GitHub: [Operational Best Practices for MAS TRMG June 2013](#).

## Operational Best Practices for Monitoring

This pack contains AWS Config rules based on monitoring within AWS. This Conformance Pack has been designed for compatibility with the majority of AWS regions and to not require setting of any Parameters. Additional managed rules that require parameters to be set for your environment and/or for your specific region can be found at: [List of AWS Config Managed Rules](#).

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

See Parameters section for names and descriptions of required parameters.

The template is available on GitHub: [Operational Best Practices for Monitoring](#).

## Operational Best Practices for NBC TRMG

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the National Bank of Cambodia's (NBC) Technology Risk Management (TRM) Guidelines framework and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more NBC TRM Guideline. An NBC TRM Guideline can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This sample conformance pack template contains mappings to controls within the National Bank of Cambodia's (NBC) Technology Risk Management (TRM) Guidelines framework, which can be accessed here: [National Bank of Cambodia: Technology Risk Management Guidelines](#).

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(d)	d) Among the important controls that need to be considered are: - A systematic process of applying and authorising the creation of user IDs and the access control matrix - Conducting a risk assessment and granting access rights based on the same. - Implementation of role-based access control designed to ensure effective segregation of duties - Changing	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.

Control ID	Control Description	AWS Config Rule	Guidance
	<p>default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contract</p> <ul style="list-style-type: none"><li>- Processes to notify in a timely manner the information security function regarding user additions, deletions and role changes -</li><li>Periodic reconciliation of user IDs in a system and actual users required to have access and deletion of any unnecessary IDs, if any</li><li>- Auditing, logging and monitoring of access to IT assets by all users and</li><li>- Considering deactivating user IDs of users of critical applications who are on prolonged leave</li></ul>		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(d)	<p>d) Among the important controls that need to be considered are:</p> <ul style="list-style-type: none"><li>- A systematic process of applying and authorising the creation of user IDs and the access control matrix</li><li>- Conducting a risk assessment and granting access rights based on the same.</li><li>- Implementation of role-based access control designed to ensure effective segregation of duties</li><li>- Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts</li><li>- Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contract</li><li>- Processes to notify in a timely manner the information security function regarding user additions, deletions and role changes</li><li>- Periodic reconciliation of user IDs in a system and actual users required to have access and deletion of any unnecessary IDs, if any</li><li>- Auditing, logging and monitoring of access to IT assets by all users and</li><li>- Considering deactivating user IDs of users of critical applications who are on prolonged leave</li></ul>	<p><a href="#">api-gw-execution-logging-enabled (p. 111)</a></p>	<p>API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(d)	<p>d) Among the important controls that need to be considered are:</p> <ul style="list-style-type: none"> <li>- A systematic process of applying and authorising the creation of user IDs and the access control matrix</li> <li>- Conducting a risk assessment and granting access rights based on the same.</li> <li>- Implementation of role-based access control designed to ensure effective segregation of duties</li> <li>- Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts</li> <li>- Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contract</li> <li>- Processes to notify in a timely manner the information security function regarding user additions, deletions and role changes</li> <li>- Periodic reconciliation of user IDs in a system and actual users required to have access and deletion of any unnecessary IDs, if any</li> <li>- Auditing, logging and monitoring of access to IT assets by all users and</li> <li>- Considering de-activating user IDs of users of critical applications who are on prolonged leave</li> </ul>	<p><a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a></p>	<p>Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(d)	<p>d) Among the important controls that need to be considered are:</p> <ul style="list-style-type: none"> <li>- A systematic process of applying and authorising the creation of user IDs and the access control matrix</li> <li>- Conducting a risk assessment and granting access rights based on the same.</li> <li>- Implementation of role-based access control designed to ensure effective segregation of duties</li> <li>- Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts</li> <li>- Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contract</li> <li>- Processes to notify in a timely manner the information security function regarding user additions, deletions and role changes</li> <li>- Periodic reconciliation of user IDs in a system and actual users required to have access and deletion of any unnecessary IDs, if any</li> <li>- Auditing, logging and monitoring of access to IT assets by all users and</li> <li>- Considering de-activating user IDs of users of critical applications who are on prolonged leave</li> </ul>	<p><a href="#">cloudtrail-enabled (p. 121)</a></p>	<p>AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(d)	<p>d) Among the important controls that need to be considered are:</p> <ul style="list-style-type: none"> <li>- A systematic process of applying and authorising the creation of user IDs and the access control matrix</li> <li>- Conducting a risk assessment and granting access rights based on the same.</li> <li>- Implementation of role-based access control designed to ensure effective segregation of duties</li> <li>- Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts</li> <li>- Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contract</li> <li>- Processes to notify in a timely manner the information security function regarding user additions, deletions and role changes</li> <li>- Periodic reconciliation of user IDs in a system and actual users required to have access and deletion of any unnecessary IDs, if any</li> <li>- Auditing, logging and monitoring of access to IT assets by all users and</li> <li>- Considering de-activating user IDs of users of critical applications who are on prolonged leave</li> </ul>	<p><a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a></p>	<p>The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(d)	<p>d) Among the important controls that need to be considered are:</p> <ul style="list-style-type: none"> <li>- A systematic process of applying and authorising the creation of user IDs and the access control matrix</li> <li>- Conducting a risk assessment and granting access rights based on the same.</li> <li>- Implementation of role-based access control designed to ensure effective segregation of duties</li> <li>- Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts</li> <li>- Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contract</li> <li>- Processes to notify in a timely manner the information security function regarding user additions, deletions and role changes</li> <li>- Periodic reconciliation of user IDs in a system and actual users required to have access and deletion of any unnecessary IDs, if any</li> <li>- Auditing, logging and monitoring of access to IT assets by all users and</li> <li>- Considering de-activating user IDs of users of critical applications who are on prolonged leave</li> </ul>	<p><a href="#">cloudwatch-alarm-action-check (p. 119)</a></p>	<p>Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(d)	<p>d) Among the important controls that need to be considered are:</p> <ul style="list-style-type: none"><li>- A systematic process of applying and authorising the creation of user IDs and the access control matrix</li><li>- Conducting a risk assessment and granting access rights based on the same.</li><li>- Implementation of role-based access control designed to ensure effective segregation of duties</li><li>- Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts</li><li>- Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contract</li><li>- Processes to notify in a timely manner the information security function regarding user additions, deletions and role changes</li><li>- Periodic reconciliation of user IDs in a system and actual users required to have access and deletion of any unnecessary IDs, if any</li><li>- Auditing, logging and monitoring of access to IT assets by all users and</li><li>- Considering deactivating user IDs of users of critical applications who are on prolonged leave</li></ul>	<p><a href="#">elb-logging-enabled (p. 144)</a></p>	<p>Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(d)	<p>d) Among the important controls that need to be considered are:</p> <ul style="list-style-type: none"><li>- A systematic process of applying and authorising the creation of user IDs and the access control matrix</li><li>- Conducting a risk assessment and granting access rights based on the same.</li><li>- Implementation of role-based access control designed to ensure effective segregation of duties</li><li>- Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts</li><li>- Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contract</li><li>- Processes to notify in a timely manner the information security function regarding user additions, deletions and role changes</li><li>- Periodic reconciliation of user IDs in a system and actual users required to have access and deletion of any unnecessary IDs, if any</li><li>- Auditing, logging and monitoring of access to IT assets by all users and</li><li>- Considering deactivating user IDs of users of critical applications who are on prolonged leave</li></ul>	<p><a href="#">guardduty-enabled-centralized (p. 152)</a></p>	<p>Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(d)	<p>d) Among the important controls that need to be considered are:</p> <ul style="list-style-type: none"> <li>- A systematic process of applying and authorising the creation of user IDs and the access control matrix</li> <li>- Conducting a risk assessment and granting access rights based on the same.</li> <li>- Implementation of role-based access control designed to ensure effective segregation of duties</li> <li>- Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts</li> <li>- Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contract</li> <li>- Processes to notify in a timely manner the information security function regarding user additions, deletions and role changes</li> <li>- Periodic reconciliation of user IDs in a system and actual users required to have access and deletion of any unnecessary IDs, if any</li> <li>- Auditing, logging and monitoring of access to IT assets by all users and</li> <li>- Considering deactivating user IDs of users of critical applications who are on prolonged leave</li> </ul>	<p><a href="#">lambda-dlq-check (p. 161)</a></p>	<p>Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(d)	<p>d) Among the important controls that need to be considered are:</p> <ul style="list-style-type: none"> <li>- A systematic process of applying and authorising the creation of user IDs and the access control matrix</li> <li>- Conducting a risk assessment and granting access rights based on the same.</li> <li>- Implementation of role-based access control designed to ensure effective segregation of duties</li> <li>- Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts</li> <li>- Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contract</li> <li>- Processes to notify in a timely manner the information security function regarding user additions, deletions and role changes</li> <li>- Periodic reconciliation of user IDs in a system and actual users required to have access and deletion of any unnecessary IDs, if any</li> <li>- Auditing, logging and monitoring of access to IT assets by all users and</li> <li>- Considering de-activating user IDs of users of critical applications who are on prolonged leave</li> </ul>	<p><a href="#">multi-region-cloudtrail-enabled (p. 163)</a></p>	<p>AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(d)	<p>d) Among the important controls that need to be considered are:</p> <ul style="list-style-type: none"> <li>- A systematic process of applying and authorising the creation of user IDs and the access control matrix</li> <li>- Conducting a risk assessment and granting access rights based on the same.</li> <li>- Implementation of role-based access control designed to ensure effective segregation of duties</li> <li>- Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts</li> <li>- Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contract</li> <li>- Processes to notify in a timely manner the information security function regarding user additions, deletions and role changes</li> <li>- Periodic reconciliation of user IDs in a system and actual users required to have access and deletion of any unnecessary IDs, if any</li> <li>- Auditing, logging and monitoring of access to IT assets by all users and</li> <li>- Considering deactivating user IDs of users of critical applications who are on prolonged leave</li> </ul>	<p><a href="#">s3-bucket-logging-enabled (p. 177)</a></p>	<p>Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(d)	<p>d) Among the important controls that need to be considered are:</p> <ul style="list-style-type: none"> <li>- A systematic process of applying and authorising the creation of user IDs and the access control matrix</li> <li>- Conducting a risk assessment and granting access rights based on the same.</li> <li>- Implementation of role-based access control designed to ensure effective segregation of duties</li> <li>- Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts</li> <li>- Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contract</li> <li>- Processes to notify in a timely manner the information security function regarding user additions, deletions and role changes</li> <li>- Periodic reconciliation of user IDs in a system and actual users required to have access and deletion of any unnecessary IDs, if any</li> <li>- Auditing, logging and monitoring of access to IT assets by all users and</li> <li>- Considering de-activating user IDs of users of critical applications who are on prolonged leave</li> </ul>	<p><a href="#">securityhub-enabled (p. 186)</a></p>	<p>AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(d)	<p>d) Among the important controls that need to be considered are:</p> <ul style="list-style-type: none"><li>- A systematic process of applying and authorising the creation of user IDs and the access control matrix</li><li>- Conducting a risk assessment and granting access rights based on the same.</li><li>- Implementation of role-based access control designed to ensure effective segregation of duties</li><li>- Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts</li><li>- Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contract</li><li>- Processes to notify in a timely manner the information security function regarding user additions, deletions and role changes</li><li>- Periodic reconciliation of user IDs in a system and actual users required to have access and deletion of any unnecessary IDs, if any</li><li>- Auditing, logging and monitoring of access to IT assets by all users and</li><li>- Considering deactivating user IDs of users of critical applications who are on prolonged leave</li></ul>	<p><a href="#">vpc-flow-logs-enabled (p. 188)</a></p>	<p>The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(d)	<p>d) Among the important controls that need to be considered are:</p> <ul style="list-style-type: none"> <li>- A systematic process of applying and authorising the creation of user IDs and the access control matrix</li> <li>- Conducting a risk assessment and granting access rights based on the same.</li> <li>- Implementation of role-based access control designed to ensure effective segregation of duties</li> <li>- Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts</li> <li>- Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contract</li> <li>- Processes to notify in a timely manner the information security function regarding user additions, deletions and role changes</li> <li>- Periodic reconciliation of user IDs in a system and actual users required to have access and deletion of any unnecessary IDs, if any</li> <li>- Auditing, logging and monitoring of access to IT assets by all users and</li> <li>- Considering de-activating user IDs of users of critical applications who are on prolonged leave</li> </ul>	<p><a href="#">cw-loggroup-retention-period-check (p. 125)</a></p>	<p>Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(d)	<p>d) Among the important controls that need to be considered are:</p> <ul style="list-style-type: none"><li>- A systematic process of applying and authorising the creation of user IDs and the access control matrix</li><li>- Conducting a risk assessment and granting access rights based on the same.</li><li>- Implementation of role-based access control designed to ensure effective segregation of duties</li><li>- Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts</li><li>- Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contract</li><li>- Processes to notify in a timely manner the information security function regarding user additions, deletions and role changes</li><li>- Periodic reconciliation of user IDs in a system and actual users required to have access and deletion of any unnecessary IDs, if any</li><li>- Auditing, logging and monitoring of access to IT assets by all users and</li><li>- Considering deactivating user IDs of users of critical applications who are on prolonged leave</li></ul>	<p><a href="#">rds-logging-enabled (p. 167)</a></p>	<p>To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(d)	<p>d) Among the important controls that need to be considered are:</p> <ul style="list-style-type: none"> <li>- A systematic process of applying and authorising the creation of user IDs and the access control matrix</li> <li>- Conducting a risk assessment and granting access rights based on the same.</li> <li>- Implementation of role-based access control designed to ensure effective segregation of duties</li> <li>- Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts</li> <li>- Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contract</li> <li>- Processes to notify in a timely manner the information security function regarding user additions, deletions and role changes</li> <li>- Periodic reconciliation of user IDs in a system and actual users required to have access and deletion of any unnecessary IDs, if any</li> <li>- Auditing, logging and monitoring of access to IT assets by all users and</li> <li>- Considering deactivating user IDs of users of critical applications who are on prolonged leave</li> </ul>	<p><a href="#">wafv2-logging-enabled (p. 190)</a></p>	<p>To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(d)	<p>d) Among the important controls that need to be considered are:</p> <ul style="list-style-type: none"> <li>- A systematic process of applying and authorising the creation of user IDs and the access control matrix</li> <li>- Conducting a risk assessment and granting access rights based on the same.</li> <li>- Implementation of role-based access control designed to ensure effective segregation of duties</li> <li>- Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts</li> <li>- Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contract</li> <li>- Processes to notify in a timely manner the information security function regarding user additions, deletions and role changes</li> <li>- Periodic reconciliation of user IDs in a system and actual users required to have access and deletion of any unnecessary IDs, if any</li> <li>- Auditing, logging and monitoring of access to IT assets by all users and</li> <li>- Considering deactivating user IDs of users of critical applications who are on prolonged leave</li> </ul>	<p><a href="#">redshift-cluster-configuration-check (p. 170)</a></p>	<p>To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(d)	<p>d) Among the important controls that need to be considered are:</p> <ul style="list-style-type: none"> <li>- A systematic process of applying and authorising the creation of user IDs and the access control matrix</li> <li>- Conducting a risk assessment and granting access rights based on the same.</li> <li>- Implementation of role-based access control designed to ensure effective segregation of duties</li> <li>- Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts</li> <li>- Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contract</li> <li>- Processes to notify in a timely manner the information security function regarding user additions, deletions and role changes</li> <li>- Periodic reconciliation of user IDs in a system and actual users required to have access and deletion of any unnecessary IDs, if any</li> <li>- Auditing, logging and monitoring of access to IT assets by all users and</li> <li>- Considering de-activating user IDs of users of critical applications who are on prolonged leave</li> </ul>	<p><a href="#">iam-user-unused-credentials-check (p. 159)</a></p>	<p>AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(h)	<p>h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered:</p> <ul style="list-style-type: none"> <li>- Implementing two-factor authentication for privileged users</li> <li>- Instituting strong controls over remote access by privileged users</li> <li>- Restricting the number of privileged users</li> <li>- Granting privileged access on a 'need-to-have' or 'need-to-do' basis</li> <li>- Maintaining audit logging of system activities performed by privileged users</li> <li>- Ensuring that privileged users do not have access to systems logs in which their activities are being captured</li> <li>- Conducting regular audit or management review of the logs</li> <li>- Prohibiting sharing of privileged IDs and their access codes</li> <li>- Disallowing vendors</li> </ul>	<a href="#">access-keys-rotated (p. 107)</a>	<p>The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	and contractors from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup data from unauthorised access		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(h)	<p>h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered:</p> <ul style="list-style-type: none"> <li>- Implementing two-factor authentication for privileged users</li> <li>- Instituting strong controls over remote access by privileged users</li> <li>- Restricting the number of privileged users</li> <li>- Granting privileged access on a 'need-to-have' or 'need-to-do' basis</li> <li>- Maintaining audit logging of system activities performed by privileged users</li> <li>- Ensuring that privileged users do not have access to systems logs in which their activities are being captured</li> <li>- Conducting regular audit or management review of the logs</li> <li>- Prohibiting sharing of privileged IDs and their access codes</li> <li>- Disallowing vendors</li> </ul>	<a href="#">efs-encrypted-check (p. 138)</a>	<p>Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).</p>

Control ID	Control Description	AWS Config Rule	Guidance
	and contractors from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup data from unauthorised access		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(h)	<p>h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered:</p> <ul style="list-style-type: none"> <li>- Implementing two-factor authentication for privileged users</li> <li>- Instituting strong controls over remote access by privileged users</li> <li>- Restricting the number of privileged users</li> <li>- Granting privileged access on a 'need-to-have' or 'need-to-do' basis</li> <li>- Maintaining audit logging of system activities performed by privileged users</li> <li>- Ensuring that privileged users do not have access to systems logs in which their activities are being captured</li> <li>- Conducting regular audit or management review of the logs</li> <li>- Prohibiting sharing of privileged IDs and their access codes</li> <li>- Disallowing vendors</li> </ul>	<p><a href="#">encrypted-volumes (p. 146)</a></p>	<p>Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	and contractors from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup data from unauthorised access		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(h)	<p>h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered:</p> <ul style="list-style-type: none"> <li>- Implementing two-factor authentication for privileged users</li> <li>- Instituting strong controls over remote access by privileged users</li> <li>- Restricting the number of privileged users</li> <li>- Granting privileged access on a 'need-to-have' or 'need-to-do' basis</li> <li>- Maintaining audit logging of system activities performed by privileged users</li> <li>- Ensuring that privileged users do not have access to systems logs in which their activities are being captured</li> <li>- Conducting regular audit or management review of the logs</li> <li>- Prohibiting sharing of privileged IDs and their access codes</li> <li>- Disallowing vendors</li> </ul>	<a href="#">rds-storage-encrypted (p. 169)</a>	<p>To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	and contractors from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup data from unauthorised access		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(h)	<p>h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered:</p> <ul style="list-style-type: none"> <li>- Implementing two-factor authentication for privileged users</li> <li>- Instituting strong controls over remote access by privileged users</li> <li>- Restricting the number of privileged users</li> <li>- Granting privileged access on a 'need-to-have' or 'need-to-do' basis</li> <li>- Maintaining audit logging of system activities performed by privileged users</li> <li>- Ensuring that privileged users do not have access to systems logs in which their activities are being captured</li> <li>- Conducting regular audit or management review of the logs</li> <li>- Prohibiting sharing of privileged IDs and their access codes</li> <li>- Disallowing vendors</li> </ul>	<a href="#">ec2-ebs-encryption-by-default (p. 131)</a>	<p>To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	and contractors from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup data from unauthorised access		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(h)	<p>h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered:</p> <ul style="list-style-type: none"> <li>- Implementing two-factor authentication for privileged users</li> <li>- Instituting strong controls over remote access by privileged users</li> <li>- Restricting the number of privileged users</li> <li>- Granting privileged access on a 'need-to-have' or 'need-to-do' basis</li> <li>- Maintaining audit logging of system activities performed by privileged users</li> <li>- Ensuring that privileged users do not have access to systems logs in which their activities are being captured</li> <li>- Conducting regular audit or management review of the logs</li> <li>- Prohibiting sharing of privileged IDs and their access codes</li> <li>- Disallowing vendors</li> </ul>	<a href="#">rds-snapshot-encrypted (p. 168)</a>	<p>Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	and contractors from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup data from unauthorised access		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(h)	<p>h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered:</p> <ul style="list-style-type: none"> <li>- Implementing two-factor authentication for privileged users</li> <li>- Instituting strong controls over remote access by privileged users</li> <li>- Restricting the number of privileged users</li> <li>- Granting privileged access on a 'need-to-have' or 'need-to-do' basis</li> <li>- Maintaining audit logging of system activities performed by privileged users</li> <li>- Ensuring that privileged users do not have access to systems logs in which their activities are being captured</li> <li>- Conducting regular audit or management review of the logs</li> <li>- Prohibiting sharing of privileged IDs and their access codes</li> <li>- Disallowing vendors</li> </ul>	<p><a href="#">emr-kerberos-enabled (p. 145)</a></p>	<p>The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	and contractors from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup data from unauthorised access		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(h)	<p>h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered:</p> <ul style="list-style-type: none"> <li>- Implementing two-factor authentication for privileged users</li> <li>- Instituting strong controls over remote access by privileged users</li> <li>- Restricting the number of privileged users</li> <li>- Granting privileged access on a 'need-to-have' or 'need-to-do' basis</li> <li>- Maintaining audit logging of system activities performed by privileged users</li> <li>- Ensuring that privileged users do not have access to systems logs in which their activities are being captured</li> <li>- Conducting regular audit or management review of the logs</li> <li>- Prohibiting sharing of privileged IDs and their access codes</li> <li>- Disallowing vendors</li> </ul>	<p><a href="#">iam-password-policy</a> (p. 154)</p>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	and contractors from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup data from unauthorised access		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(h)	<p>h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered:</p> <ul style="list-style-type: none"> <li>- Implementing two-factor authentication for privileged users</li> <li>- Instituting strong controls over remote access by privileged users</li> <li>- Restricting the number of privileged users</li> <li>- Granting privileged access on a 'need-to-have' or 'need-to-do' basis</li> <li>- Maintaining audit logging of system activities performed by privileged users</li> <li>- Ensuring that privileged users do not have access to systems logs in which their activities are being captured</li> <li>- Conducting regular audit or management review of the logs</li> <li>- Prohibiting sharing of privileged IDs and their access codes</li> <li>- Disallowing vendors</li> </ul>	<p><a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a></p>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	and contractors from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup data from unauthorised access		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(h)	<p>h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered:</p> <ul style="list-style-type: none"> <li>- Implementing two-factor authentication for privileged users</li> <li>- Instituting strong controls over remote access by privileged users</li> <li>- Restricting the number of privileged users</li> <li>- Granting privileged access on a 'need-to-have' or 'need-to-do' basis</li> <li>- Maintaining audit logging of system activities performed by privileged users</li> <li>- Ensuring that privileged users do not have access to systems logs in which their activities are being captured</li> <li>- Conducting regular audit or management review of the logs</li> <li>- Prohibiting sharing of privileged IDs and their access codes</li> <li>- Disallowing vendors</li> </ul>	<a href="#">iam-root-access-key-check (p. 157)</a>	<p>Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	and contractors from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup data from unauthorised access		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(h)	<p>h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered:</p> <ul style="list-style-type: none"> <li>- Implementing two-factor authentication for privileged users</li> <li>- Instituting strong controls over remote access by privileged users</li> <li>- Restricting the number of privileged users</li> <li>- Granting privileged access on a 'need-to-have' or 'need-to-do' basis</li> <li>- Maintaining audit logging of system activities performed by privileged users</li> <li>- Ensuring that privileged users do not have access to systems logs in which their activities are being captured</li> <li>- Conducting regular audit or management review of the logs</li> <li>- Prohibiting sharing of privileged IDs and their access codes</li> <li>- Disallowing vendors</li> </ul>	<a href="#">iam-user-mfa-enabled (p. 158)</a>	<p>Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	and contractors from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup data from unauthorised access		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(h)	<p>h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered:</p> <ul style="list-style-type: none"> <li>- Implementing two-factor authentication for privileged users</li> <li>- Instituting strong controls over remote access by privileged users</li> <li>- Restricting the number of privileged users</li> <li>- Granting privileged access on a 'need-to-have' or 'need-to-do' basis</li> <li>- Maintaining audit logging of system activities performed by privileged users</li> <li>- Ensuring that privileged users do not have access to systems logs in which their activities are being captured</li> <li>- Conducting regular audit or management review of the logs</li> <li>- Prohibiting sharing of privileged IDs and their access codes</li> <li>- Disallowing vendors</li> </ul>	<a href="#">iam-user-no-policies-check (p. 158)</a>	<p>This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	and contractors from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup data from unauthorised access		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(h)	<p>h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered:</p> <ul style="list-style-type: none"> <li>- Implementing two-factor authentication for privileged users</li> <li>- Instituting strong controls over remote access by privileged users</li> <li>- Restricting the number of privileged users</li> <li>- Granting privileged access on a 'need-to-have' or 'need-to-do' basis</li> <li>- Maintaining audit logging of system activities performed by privileged users</li> <li>- Ensuring that privileged users do not have access to systems logs in which their activities are being captured</li> <li>- Conducting regular audit or management review of the logs</li> <li>- Prohibiting sharing of privileged IDs and their access codes</li> <li>- Disallowing vendors</li> </ul>	<p><a href="#">iam-user-unused-credentials-check (p. 159)</a></p>	<p>AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	and contractors from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup data from unauthorised access		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(h)	<p>h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered:</p> <ul style="list-style-type: none"> <li>- Implementing two-factor authentication for privileged users</li> <li>- Instituting strong controls over remote access by privileged users</li> <li>- Restricting the number of privileged users</li> <li>- Granting privileged access on a 'need-to-have' or 'need-to-do' basis</li> <li>- Maintaining audit logging of system activities performed by privileged users</li> <li>- Ensuring that privileged users do not have access to systems logs in which their activities are being captured</li> <li>- Conducting regular audit or management review of the logs</li> <li>- Prohibiting sharing of privileged IDs and their access codes</li> <li>- Disallowing vendors</li> </ul>	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	<p>Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	and contractors from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup data from unauthorised access		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(h)	<p>h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered:</p> <ul style="list-style-type: none"> <li>- Implementing two-factor authentication for privileged users</li> <li>- Instituting strong controls over remote access by privileged users</li> <li>- Restricting the number of privileged users</li> <li>- Granting privileged access on a 'need-to-have' or 'need-to-do' basis</li> <li>- Maintaining audit logging of system activities performed by privileged users</li> <li>- Ensuring that privileged users do not have access to systems logs in which their activities are being captured</li> <li>- Conducting regular audit or management review of the logs</li> <li>- Prohibiting sharing of privileged IDs and their access codes</li> <li>- Disallowing vendors</li> </ul>	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	<p>Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	and contractors from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup data from unauthorised access		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(h)	<p>h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered:</p> <ul style="list-style-type: none"> <li>- Implementing two-factor authentication for privileged users</li> <li>- Instituting strong controls over remote access by privileged users</li> <li>- Restricting the number of privileged users</li> <li>- Granting privileged access on a 'need-to-have' or 'need-to-do' basis</li> <li>- Maintaining audit logging of system activities performed by privileged users</li> <li>- Ensuring that privileged users do not have access to systems logs in which their activities are being captured</li> <li>- Conducting regular audit or management review of the logs</li> <li>- Prohibiting sharing of privileged IDs and their access codes</li> <li>- Disallowing vendors</li> </ul>	<a href="#">root-account-mfa-enabled (p. 175)</a>	<p>Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	and contractors from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup data from unauthorised access		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(h)	<p>h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered:</p> <ul style="list-style-type: none"> <li>- Implementing two-factor authentication for privileged users</li> <li>- Instituting strong controls over remote access by privileged users</li> <li>- Restricting the number of privileged users</li> <li>- Granting privileged access on a 'need-to-have' or 'need-to-do' basis</li> <li>- Maintaining audit logging of system activities performed by privileged users</li> <li>- Ensuring that privileged users do not have access to systems logs in which their activities are being captured</li> <li>- Conducting regular audit or management review of the logs</li> <li>- Prohibiting sharing of privileged IDs and their access codes</li> <li>- Disallowing vendors</li> </ul>	<a href="#">iam-no-inline-policy-check (p. 154)</a>	<p>Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	and contractors from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup data from unauthorised access		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(h)	<p>h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered:</p> <ul style="list-style-type: none"> <li>- Implementing two-factor authentication for privileged users</li> <li>- Instituting strong controls over remote access by privileged users</li> <li>- Restricting the number of privileged users</li> <li>- Granting privileged access on a 'need-to-have' or 'need-to-do' basis</li> <li>- Maintaining audit logging of system activities performed by privileged users</li> <li>- Ensuring that privileged users do not have access to systems logs in which their activities are being captured</li> <li>- Conducting regular audit or management review of the logs</li> <li>- Prohibiting sharing of privileged IDs and their access codes</li> <li>- Disallowing vendors</li> </ul>	<p><a href="#">api-gw-execution-logging-enabled</a> (p. 111)</p>	<p>API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	and contractors from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup data from unauthorised access		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(h)	<p>h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered:</p> <ul style="list-style-type: none"> <li>- Implementing two-factor authentication for privileged users</li> <li>- Instituting strong controls over remote access by privileged users</li> <li>- Restricting the number of privileged users</li> <li>- Granting privileged access on a 'need-to-have' or 'need-to-do' basis</li> <li>- Maintaining audit logging of system activities performed by privileged users</li> <li>- Ensuring that privileged users do not have access to systems logs in which their activities are being captured</li> <li>- Conducting regular audit or management review of the logs</li> <li>- Prohibiting sharing of privileged IDs and their access codes</li> <li>- Disallowing vendors</li> </ul>	<p><a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a></p>	<p>Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	and contractors from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup data from unauthorised access		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(h)	<p>h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered:</p> <ul style="list-style-type: none"> <li>- Implementing two-factor authentication for privileged users</li> <li>- Instituting strong controls over remote access by privileged users</li> <li>- Restricting the number of privileged users</li> <li>- Granting privileged access on a 'need-to-have' or 'need-to-do' basis</li> <li>- Maintaining audit logging of system activities performed by privileged users</li> <li>- Ensuring that privileged users do not have access to systems logs in which their activities are being captured</li> <li>- Conducting regular audit or management review of the logs</li> <li>- Prohibiting sharing of privileged IDs and their access codes</li> <li>- Disallowing vendors</li> </ul>	<a href="#">cloudtrail-enabled (p. 121)</a>	<p>AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	and contractors from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup data from unauthorised access		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(h)	<p>h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered:</p> <ul style="list-style-type: none"> <li>- Implementing two-factor authentication for privileged users</li> <li>- Instituting strong controls over remote access by privileged users</li> <li>- Restricting the number of privileged users</li> <li>- Granting privileged access on a 'need-to-have' or 'need-to-do' basis</li> <li>- Maintaining audit logging of system activities performed by privileged users</li> <li>- Ensuring that privileged users do not have access to systems logs in which their activities are being captured</li> <li>- Conducting regular audit or management review of the logs</li> <li>- Prohibiting sharing of privileged IDs and their access codes</li> <li>- Disallowing vendors</li> </ul>	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	<p>The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	and contractors from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup data from unauthorised access		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(h)	<p>h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered:</p> <ul style="list-style-type: none"> <li>- Implementing two-factor authentication for privileged users</li> <li>- Instituting strong controls over remote access by privileged users</li> <li>- Restricting the number of privileged users</li> <li>- Granting privileged access on a 'need-to-have' or 'need-to-do' basis</li> <li>- Maintaining audit logging of system activities performed by privileged users</li> <li>- Ensuring that privileged users do not have access to systems logs in which their activities are being captured</li> <li>- Conducting regular audit or management review of the logs</li> <li>- Prohibiting sharing of privileged IDs and their access codes</li> <li>- Disallowing vendors</li> </ul>	<p><a href="#">elb-logging-enabled (p. 144)</a></p>	<p>Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	and contractors from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup data from unauthorised access		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(h)	<p>h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered:</p> <ul style="list-style-type: none"> <li>- Implementing two-factor authentication for privileged users</li> <li>- Instituting strong controls over remote access by privileged users</li> <li>- Restricting the number of privileged users</li> <li>- Granting privileged access on a 'need-to-have' or 'need-to-do' basis</li> <li>- Maintaining audit logging of system activities performed by privileged users</li> <li>- Ensuring that privileged users do not have access to systems logs in which their activities are being captured</li> <li>- Conducting regular audit or management review of the logs</li> <li>- Prohibiting sharing of privileged IDs and their access codes</li> <li>- Disallowing vendors</li> </ul>	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	<p>AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	and contractors from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup data from unauthorised access		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(h)	<p>h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered:</p> <ul style="list-style-type: none"> <li>- Implementing two-factor authentication for privileged users</li> <li>- Instituting strong controls over remote access by privileged users</li> <li>- Restricting the number of privileged users</li> <li>- Granting privileged access on a 'need-to-have' or 'need-to-do' basis</li> <li>- Maintaining audit logging of system activities performed by privileged users</li> <li>- Ensuring that privileged users do not have access to systems logs in which their activities are being captured</li> <li>- Conducting regular audit or management review of the logs</li> <li>- Prohibiting sharing of privileged IDs and their access codes</li> <li>- Disallowing vendors</li> </ul>	<p><a href="#">s3-bucket-logging-enabled (p. 177)</a></p>	<p>Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	and contractors from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup data from unauthorised access		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(h)	<p>h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered:</p> <ul style="list-style-type: none"> <li>- Implementing two-factor authentication for privileged users</li> <li>- Instituting strong controls over remote access by privileged users</li> <li>- Restricting the number of privileged users</li> <li>- Granting privileged access on a 'need-to-have' or 'need-to-do' basis</li> <li>- Maintaining audit logging of system activities performed by privileged users</li> <li>- Ensuring that privileged users do not have access to systems logs in which their activities are being captured</li> <li>- Conducting regular audit or management review of the logs</li> <li>- Prohibiting sharing of privileged IDs and their access codes</li> <li>- Disallowing vendors</li> </ul>	<p><a href="#">vpc-flow-logs-enabled (p. 188)</a></p>	<p>The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	and contractors from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup data from unauthorised access		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(h)	<p>h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered:</p> <ul style="list-style-type: none"> <li>- Implementing two-factor authentication for privileged users</li> <li>- Instituting strong controls over remote access by privileged users</li> <li>- Restricting the number of privileged users</li> <li>- Granting privileged access on a 'need-to-have' or 'need-to-do' basis</li> <li>- Maintaining audit logging of system activities performed by privileged users</li> <li>- Ensuring that privileged users do not have access to systems logs in which their activities are being captured</li> <li>- Conducting regular audit or management review of the logs</li> <li>- Prohibiting sharing of privileged IDs and their access codes</li> <li>- Disallowing vendors</li> </ul>	<a href="#">cw-loggroup-retention-period-check (p. 125)</a>	<p>Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	and contractors from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup data from unauthorised access		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(h)	<p>h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered:</p> <ul style="list-style-type: none"> <li>- Implementing two-factor authentication for privileged users</li> <li>- Instituting strong controls over remote access by privileged users</li> <li>- Restricting the number of privileged users</li> <li>- Granting privileged access on a 'need-to-have' or 'need-to-do' basis</li> <li>- Maintaining audit logging of system activities performed by privileged users</li> <li>- Ensuring that privileged users do not have access to systems logs in which their activities are being captured</li> <li>- Conducting regular audit or management review of the logs</li> <li>- Prohibiting sharing of privileged IDs and their access codes</li> <li>- Disallowing vendors</li> </ul>	<p><a href="#">rds-logging-enabled (p. 167)</a></p>	<p>To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	and contractors from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup data from unauthorised access		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(h)	<p>h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered:</p> <ul style="list-style-type: none"> <li>- Implementing two-factor authentication for privileged users</li> <li>- Instituting strong controls over remote access by privileged users</li> <li>- Restricting the number of privileged users</li> <li>- Granting privileged access on a 'need-to-have' or 'need-to-do' basis</li> <li>- Maintaining audit logging of system activities performed by privileged users</li> <li>- Ensuring that privileged users do not have access to systems logs in which their activities are being captured</li> <li>- Conducting regular audit or management review of the logs</li> <li>- Prohibiting sharing of privileged IDs and their access codes</li> <li>- Disallowing vendors</li> </ul>	<p><a href="#">wafv2-logging-enabled (p. 190)</a></p>	<p>To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	and contractors from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup data from unauthorised access		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1(h)	<p>h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered:</p> <ul style="list-style-type: none"> <li>- Implementing two-factor authentication for privileged users</li> <li>- Instituting strong controls over remote access by privileged users</li> <li>- Restricting the number of privileged users</li> <li>- Granting privileged access on a 'need-to-have' or 'need-to-do' basis</li> <li>- Maintaining audit logging of system activities performed by privileged users</li> <li>- Ensuring that privileged users do not have access to systems logs in which their activities are being captured</li> <li>- Conducting regular audit or management review of the logs</li> <li>- Prohibiting sharing of privileged IDs and their access codes</li> <li>- Disallowing vendors</li> </ul>	<p><a href="#">redshift-cluster-configuration-check (p. 170)</a></p>	<p>To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	<p>and contractors from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup data from unauthorised access</p>		
3.1.2(a)	<p>a) The BFI should install network security devices, such as firewalls, anti-virus/anti-malware software as well as intrusion detection and prevention systems, at critical junctures of its IT infrastructure, to protect the network perimeters.</p>	<p><a href="#">alb-waf-enabled (p. 109)</a></p>	<p>Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.</p>
3.1.2(a)	<p>a) The BFI should install network security devices, such as firewalls, anti-virus/anti-malware software as well as intrusion detection and prevention systems, at critical junctures of its IT infrastructure, to protect the network perimeters.</p>	<p><a href="#">guardduty-enabled-centralized (p. 152)</a></p>	<p>Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<p><a href="#">acm-certificate-expiration-check (p. 108)</a></p>	<p>Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<p><a href="#">alb-http-to-https-redirection-check (p. 109)</a></p>	<p>To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<p><a href="#">elb-acm-certificate-required (p. 143)</a></p>	<p>Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<a href="#">redshift-require-tls-ssl (p. 172)</a>	<p>Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<p><a href="#">s3-bucket-ssl-requests-only (p. 181)</a></p>	<p>To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	<p>Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<p><a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a></p>	<p>Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"><li>- Responsibilities and procedures for the management of networking equipment should be established</li><li>- Operational responsibility for networks should be separated from computer operations where appropriate</li><li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li><li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li><li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li><li>- Systems on the network should be authenticated and</li></ul>	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	<p>Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"><li>- Responsibilities and procedures for the management of networking equipment should be established</li><li>- Operational responsibility for networks should be separated from computer operations where appropriate</li><li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li><li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li><li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li><li>- Systems on the network should be authenticated and</li></ul>	<p><a href="#">api-gw-execution-logging-enabled (p. 111)</a></p>	<p>API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"><li>- Responsibilities and procedures for the management of networking equipment should be established</li><li>- Operational responsibility for networks should be separated from computer operations where appropriate</li><li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li><li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li><li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li><li>- Systems on the network should be authenticated and</li></ul>	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	<p>Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<a href="#">cloudtrail-enabled (p. 121)</a>	<p>AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	<p>The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	<p>Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<p><a href="#">elb-logging-enabled (p. 144)</a></p>	<p>Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<a href="#">guardduty-enabled-centralized (p. 152)</a>	<p>Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<a href="#">lambda-dlq-check (p. 161)</a>	<p>Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	<p>AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<p><a href="#">s3-bucket-logging-enabled (p. 177)</a></p>	<p>Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<a href="#">securityhub-enabled (p. 186)</a>	<p>AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"><li>- Responsibilities and procedures for the management of networking equipment should be established</li><li>- Operational responsibility for networks should be separated from computer operations where appropriate</li><li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li><li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li><li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li><li>- Systems on the network should be authenticated and</li></ul>	<a href="#">rds-logging-enabled (p. 167)</a>	<p>To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<a href="#">wafv2-logging-enabled (p. 190)</a>	<p>To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<p><a href="#">redshift-cluster-configuration-check (p. 170)</a></p>	<p>To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<p><a href="#">dms-replication-not-public (p. 127)</a></p>	<p>Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<p><a href="#">ebs-snapshot-public-restorable-check (p. 131)</a></p>	<p>Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"><li>- Responsibilities and procedures for the management of networking equipment should be established</li><li>- Operational responsibility for networks should be separated from computer operations where appropriate</li><li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li><li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li><li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li><li>- Systems on the network should be authenticated and</li></ul>	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	<p>Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	<p>Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<p><a href="#">emr-master-no-public-ip (p. 146)</a></p>	<p>Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<a href="#">restricted-ssh (p. 159)</a>	<p>Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<p><a href="#">ec2-instances-in-vpc (p. 159)</a></p>	<p>Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<p><a href="#">internet-gateway-authorized-vpc-only (p. 160)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	<p>Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<a href="#">lambda-inside-vpc (p. 162)</a>	<p>Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<a href="#">rds-instance-public-access-check (p. 166)</a>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"><li>- Responsibilities and procedures for the management of networking equipment should be established</li><li>- Operational responsibility for networks should be separated from computer operations where appropriate</li><li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li><li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li><li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li><li>- Systems on the network should be authenticated and</li></ul>	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<a href="#">restricted-common-ports (p. 174)</a>	<p>Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1</p> <ul style="list-style-type: none"> <li>- blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333).</li> </ul> <p>The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<p><a href="#">s3-account-level-public-access-blocks (p. 175)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	<p>Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<p><a href="#">s3-bucket-public-write-prohibited (p. 180)</a></p>	<p>Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<p><a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<a href="#">vpc-default-security-group-closed (p. 188)</a>	<p>Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(c)	<p>c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:</p> <ul style="list-style-type: none"> <li>- Responsibilities and procedures for the management of networking equipment should be established</li> <li>- Operational responsibility for networks should be separated from computer operations where appropriate</li> <li>- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks.</li> <li>- Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security</li> <li>- Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure</li> <li>- Systems on the network should be authenticated and</li> </ul>	<p><a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	- Untrusted system connections to the network should be restricted		
3.1.2(e)	e) Network services can range from simple unmanaged bandwidth to sophisticated services such as VPN, Voice over IP, VSAT, etc. Security features of network services should be: - Technology applied for security of network services, such as authentication, encryption and network connection controls - Technical parameters required for secured connection with the network services in accordance with the security and network connection rules and - Procedures for the network service usage to restrict access to network services or applications, where necessary	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(e)	<p>e) Network services can range from simple unmanaged bandwidth to sophisticated services such as VPN, Voice over IP, VSAT, etc. Security features of network services should be:</p> <ul style="list-style-type: none"><li>- Technology applied for security of network services, such as authentication, encryption and network connection controls</li><li>- Technical parameters required for secured connection with the network services in accordance with the security and network connection rules and</li><li>- Procedures for the network service usage to restrict access to network services or applications, where necessary</li></ul>	<p><a href="#">emr-kerberos-enabled (p. 145)</a></p>	<p>The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(e)	<p>e) Network services can range from simple unmanaged bandwidth to sophisticated services such as VPN, Voice over IP, VSAT, etc. Security features of network services should be:</p> <ul style="list-style-type: none"> <li>- Technology applied for security of network services, such as authentication, encryption and network connection controls</li> <li>- Technical parameters required for secured connection with the network services in accordance with the security and network connection rules and</li> <li>- Procedures for the network service usage to restrict access to network services or applications, where necessary</li> </ul>	<p><a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a></p>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.</p>
3.1.2(e)	<p>e) Network services can range from simple unmanaged bandwidth to sophisticated services such as VPN, Voice over IP, VSAT, etc. Security features of network services should be:</p> <ul style="list-style-type: none"> <li>- Technology applied for security of network services, such as authentication, encryption and network connection controls</li> <li>- Technical parameters required for secured connection with the network services in accordance with the security and network connection rules and</li> <li>- Procedures for the network service usage to restrict access to network services or applications, where necessary</li> </ul>	<p><a href="#">iam-root-access-key-check (p. 157)</a></p>	<p>Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(e)	<p>e) Network services can range from simple unmanaged bandwidth to sophisticated services such as VPN, Voice over IP, VSAT, etc. Security features of network services should be:</p> <ul style="list-style-type: none"><li>- Technology applied for security of network services, such as authentication, encryption and network connection controls</li><li>- Technical parameters required for secured connection with the network services in accordance with the security and network connection rules and</li><li>- Procedures for the network service usage to restrict access to network services or applications, where necessary</li></ul>	<p><a href="#">iam-user-group-membership-check (p. 157)</a></p>	<p>AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(e)	<p>e) Network services can range from simple unmanaged bandwidth to sophisticated services such as VPN, Voice over IP, VSAT, etc. Security features of network services should be: - Technology applied for security of network services, such as authentication, encryption and network connection controls - Technical parameters required for secured connection with the network services in accordance with the security and network connection rules and - Procedures for the network service usage to restrict access to network services or applications, where necessary</p>	<p><a href="#">iam-password-policy (p. 154)</a></p>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(e)	<p>e) Network services can range from simple unmanaged bandwidth to sophisticated services such as VPN, Voice over IP, VSAT, etc. Security features of network services should be:</p> <ul style="list-style-type: none"> <li>- Technology applied for security of network services, such as authentication, encryption and network connection controls</li> <li>- Technical parameters required for secured connection with the network services in accordance with the security and network connection rules and</li> <li>- Procedures for the network service usage to restrict access to network services or applications, where necessary</li> </ul>	<p><a href="#">iam-no-inline-policy-check (p. 154)</a></p>	<p>Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.</p>
3.1.2(e)	<p>e) Network services can range from simple unmanaged bandwidth to sophisticated services such as VPN, Voice over IP, VSAT, etc. Security features of network services should be:</p> <ul style="list-style-type: none"> <li>- Technology applied for security of network services, such as authentication, encryption and network connection controls</li> <li>- Technical parameters required for secured connection with the network services in accordance with the security and network connection rules and</li> <li>- Procedures for the network service usage to restrict access to network services or applications, where necessary</li> </ul>	<p><a href="#">iam-user-mfa-enabled (p. 158)</a></p>	<p>Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(e)	<p>e) Network services can range from simple unmanaged bandwidth to sophisticated services such as VPN, Voice over IP, VSAT, etc. Security features of network services should be: - Technology applied for security of network services, such as authentication, encryption and network connection controls - Technical parameters required for secured connection with the network services in accordance with the security and network connection rules and - Procedures for the network service usage to restrict access to network services or applications, where necessary</p>	<p><a href="#">mfa-enabled-for-iam-console-access (p. 163)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.</p>
3.1.2(e)	<p>e) Network services can range from simple unmanaged bandwidth to sophisticated services such as VPN, Voice over IP, VSAT, etc. Security features of network services should be: - Technology applied for security of network services, such as authentication, encryption and network connection controls - Technical parameters required for secured connection with the network services in accordance with the security and network connection rules and - Procedures for the network service usage to restrict access to network services or applications, where necessary</p>	<p><a href="#">root-account-hardware-mfa-enabled (p. 175)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(e)	<p>e) Network services can range from simple unmanaged bandwidth to sophisticated services such as VPN, Voice over IP, VSAT, etc. Security features of network services should be: - Technology applied for security of network services, such as authentication, encryption and network connection controls - Technical parameters required for secured connection with the network services in accordance with the security and network connection rules and - Procedures for the network service usage to restrict access to network services or applications, where necessary</p>	<p><a href="#">root-account-mfa-enabled (p. 175)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.</p>
3.1.2(e)	<p>e) Network services can range from simple unmanaged bandwidth to sophisticated services such as VPN, Voice over IP, VSAT, etc. Security features of network services should be: - Technology applied for security of network services, such as authentication, encryption and network connection controls - Technical parameters required for secured connection with the network services in accordance with the security and network connection rules and - Procedures for the network service usage to restrict access to network services or applications, where necessary</p>	<p><a href="#">alb-http-to-https-redirect-check (p. 109)</a></p>	<p>To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(e)	<p>e) Network services can range from simple unmanaged bandwidth to sophisticated services such as VPN, Voice over IP, VSAT, etc. Security features of network services should be: - Technology applied for security of network services, such as authentication, encryption and network connection controls - Technical parameters required for secured connection with the network services in accordance with the security and network connection rules and - Procedures for the network service usage to restrict access to network services or applications, where necessary</p>	<p><a href="#">elb-acm-certificate-required (p. 143)</a></p>	<p>Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.</p>
3.1.2(e)	<p>e) Network services can range from simple unmanaged bandwidth to sophisticated services such as VPN, Voice over IP, VSAT, etc. Security features of network services should be: - Technology applied for security of network services, such as authentication, encryption and network connection controls - Technical parameters required for secured connection with the network services in accordance with the security and network connection rules and - Procedures for the network service usage to restrict access to network services or applications, where necessary</p>	<p><a href="#">redshift-require-tls-ssl (p. 172)</a></p>	<p>Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(e)	<p>e) Network services can range from simple unmanaged bandwidth to sophisticated services such as VPN, Voice over IP, VSAT, etc. Security features of network services should be:</p> <ul style="list-style-type: none"> <li>- Technology applied for security of network services, such as authentication, encryption and network connection controls</li> <li>- Technical parameters required for secured connection with the network services in accordance with the security and network connection rules and</li> <li>- Procedures for the network service usage to restrict access to network services or applications, where necessary</li> </ul>	<p><a href="#">s3-bucket-ssl-requests-only (p. 181)</a></p>	<p>To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.</p>
3.1.2(e)	<p>e) Network services can range from simple unmanaged bandwidth to sophisticated services such as VPN, Voice over IP, VSAT, etc. Security features of network services should be:</p> <ul style="list-style-type: none"> <li>- Technology applied for security of network services, such as authentication, encryption and network connection controls</li> <li>- Technical parameters required for secured connection with the network services in accordance with the security and network connection rules and</li> <li>- Procedures for the network service usage to restrict access to network services or applications, where necessary</li> </ul>	<p><a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a></p>	<p>Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2(e)	<p>e) Network services can range from simple unmanaged bandwidth to sophisticated services such as VPN, Voice over IP, VSAT, etc. Security features of network services should be: - Technology applied for security of network services, such as authentication, encryption and network connection controls - Technical parameters required for secured connection with the network services in accordance with the security and network connection rules and - Procedures for the network service usage to restrict access to network services or applications, where necessary</p>	<p><a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a></p>	<p>Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.</p>
3.1.2(e)	<p>e) Network services can range from simple unmanaged bandwidth to sophisticated services such as VPN, Voice over IP, VSAT, etc. Security features of network services should be: - Technology applied for security of network services, such as authentication, encryption and network connection controls - Technical parameters required for secured connection with the network services in accordance with the security and network connection rules and - Procedures for the network service usage to restrict access to network services or applications, where necessary</p>	<p><a href="#">elb-tls-https-listeners-only (p. 145)</a></p>	<p>Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.3(e)	e) Use encryption to protect communication channels between the remote access device and the institution to restrict the risks related to network spoofing.	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.
3.1.3(e)	e) Use encryption to protect communication channels between the remote access device and the institution to restrict the risks related to network spoofing.	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
3.1.3(e)	e) Use encryption to protect communication channels between the remote access device and the institution to restrict the risks related to network spoofing.	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
3.1.3(e)	e) Use encryption to protect communication channels between the remote access device and the institution to restrict the risks related to network spoofing.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.3(e)	e) Use encryption to protect communication channels between the remote access device and the institution to restrict the risks related to network spoofing.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
3.1.3(e)	e) Use encryption to protect communication channels between the remote access device and the institution to restrict the risks related to network spoofing.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
3.1.3(e)	e) Use encryption to protect communication channels between the remote access device and the institution to restrict the risks related to network spoofing.	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
3.1.3(e)	e) Use encryption to protect communication channels between the remote access device and the institution to restrict the risks related to network spoofing.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.3(f)	f) While using TCP/IP Internet-based remote access, organisations need to establish a virtual private network over the Internet to securely communicate data packets over this public infrastructure. Further, VLANs', network segments to restrict remote access to authorised network areas and applications within the institution.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
3.1.3(f)	f) While using TCP/IP Internet-based remote access, organisations need to establish a virtual private network over the Internet to securely communicate data packets over this public infrastructure. Further, VLANs', network segments to restrict remote access to authorised network areas and applications within the institution.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
3.1.3(f)	f) While using TCP/IP Internet-based remote access, organisations need to establish a virtual private network over the Internet to securely communicate data packets over this public infrastructure. Further, VLANs', network segments to restrict remote access to authorised network areas and applications within the institution.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.3(f)	f) While using TCP/IP Internet-based remote access, organisations need to establish a virtual private network over the Internet to securely communicate data packets over this public infrastructure. Further, VLANs', network segments to restrict remote access to authorised network areas and applications within the institution.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
3.1.3(f)	f) While using TCP/IP Internet-based remote access, organisations need to establish a virtual private network over the Internet to securely communicate data packets over this public infrastructure. Further, VLANs', network segments to restrict remote access to authorised network areas and applications within the institution.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
3.1.3(f)	f) While using TCP/IP Internet-based remote access, organisations need to establish a virtual private network over the Internet to securely communicate data packets over this public infrastructure. Further, VLANs', network segments to restrict remote access to authorised network areas and applications within the institution.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.3(f)	f) While using TCP/IP Internet-based remote access, organisations need to establish a virtual private network over the Internet to securely communicate data packets over this public infrastructure. Further, VLANs, network segments to restrict remote access to authorised network areas and applications within the institution.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
3.1.3(f)	f) While using TCP/IP Internet-based remote access, organisations need to establish a virtual private network over the Internet to securely communicate data packets over this public infrastructure. Further, VLANs, network segments to restrict remote access to authorised network areas and applications within the institution.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.3(f)	f) While using TCP/IP Internet-based remote access, organisations need to establish a virtual private network over the Internet to securely communicate data packets over this public infrastructure. Further, VLANs, network segments to restrict remote access to authorised network areas and applications within the institution.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
3.1.3(f)	f) While using TCP/IP Internet-based remote access, organisations need to establish a virtual private network over the Internet to securely communicate data packets over this public infrastructure. Further, VLANs, network segments to restrict remote access to authorised network areas and applications within the institution.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.3(f)	f) While using TCP/IP Internet-based remote access, organisations need to establish a virtual private network over the Internet to securely communicate data packets over this public infrastructure. Further, VLANs', network segments to restrict remote access to authorised network areas and applications within the institution.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
3.1.3(f)	f) While using TCP/IP Internet-based remote access, organisations need to establish a virtual private network over the Internet to securely communicate data packets over this public infrastructure. Further, VLANs', network segments to restrict remote access to authorised network areas and applications within the institution.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
3.1.3(f)	f) While using TCP/IP Internet-based remote access, organisations need to establish a virtual private network over the Internet to securely communicate data packets over this public infrastructure. Further, VLANs', network segments to restrict remote access to authorised network areas and applications within the institution.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.3(f)	f) While using TCP/IP Internet-based remote access, organisations need to establish a virtual private network over the Internet to securely communicate data packets over this public infrastructure. Further, VLANs, network segments to restrict remote access to authorised network areas and applications within the institution.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
3.1.3(f)	f) While using TCP/IP Internet-based remote access, organisations need to establish a virtual private network over the Internet to securely communicate data packets over this public infrastructure. Further, VLANs, network segments to restrict remote access to authorised network areas and applications within the institution.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.3(f)	f) While using TCP/IP Internet-based remote access, organisations need to establish a virtual private network over the Internet to securely communicate data packets over this public infrastructure. Further, VLANs', network segments to restrict remote access to authorised network areas and applications within the institution.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
3.1.3(f)	f) While using TCP/IP Internet-based remote access, organisations need to establish a virtual private network over the Internet to securely communicate data packets over this public infrastructure. Further, VLANs', network segments to restrict remote access to authorised network areas and applications within the institution.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
3.1.3(f)	f) While using TCP/IP Internet-based remote access, organisations need to establish a virtual private network over the Internet to securely communicate data packets over this public infrastructure. Further, VLANs', network segments to restrict remote access to authorised network areas and applications within the institution.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.3(f)	f) While using TCP/IP Internet-based remote access, organisations need to establish a virtual private network over the Internet to securely communicate data packets over this public infrastructure. Further, VLANs, network segments to restrict remote access to authorised network areas and applications within the institution.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
3.1.3(f)	f) While using TCP/IP Internet-based remote access, organisations need to establish a virtual private network over the Internet to securely communicate data packets over this public infrastructure. Further, VLANs, network segments to restrict remote access to authorised network areas and applications within the institution.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
3.1.3(g)	g) Maintain logs for remote access communications. Logs should include the date, time, user, user location, duration, and purpose for all remote access including all activities carried out through remote access	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.3(g)	g) Maintain logs for remote access communications. Logs should include the date, time, user, user location, duration, and purpose for all remote access including all activities carried out through remote access	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
3.1.3(g)	g) Maintain logs for remote access communications. Logs should include the date, time, user, user location, duration, and purpose for all remote access including all activities carried out through remote access	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
3.1.3(g)	g) Maintain logs for remote access communications. Logs should include the date, time, user, user location, duration, and purpose for all remote access including all activities carried out through remote access	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.3(g)	g) Maintain logs for remote access communications. Logs should include the date, time, user, user location, duration, and purpose for all remote access including all activities carried out through remote access	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
3.1.3(g)	g) Maintain logs for remote access communications. Logs should include the date, time, user, user location, duration, and purpose for all remote access including all activities carried out through remote access	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.3(g)	g) Maintain logs for remote access communications. Logs should include the date, time, user, user location, duration, and purpose for all remote access including all activities carried out through remote access	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
3.1.3(g)	g) Maintain logs for remote access communications. Logs should include the date, time, user, user location, duration, and purpose for all remote access including all activities carried out through remote access	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
3.1.3(g)	g) Maintain logs for remote access communications. Logs should include the date, time, user, user location, duration, and purpose for all remote access including all activities carried out through remote access	<a href="#">cw-loggroup-retention-period-check (p. 125)</a>	Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.3(g)	g) Maintain logs for remote access communications. Logs should include the date, time, user, user location, duration, and purpose for all remote access including all activities carried out through remote access	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
3.1.3(g)	g) Maintain logs for remote access communications. Logs should include the date, time, user, user location, duration, and purpose for all remote access including all activities carried out through remote access	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.3(g)	g) Maintain logs for remote access communications. Logs should include the date, time, user, user location, duration, and purpose for all remote access including all activities carried out through remote access	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
3.1.3(i)	i) Enforce two-factor authentication process for remote access (e.g., PIN based token card with a one-time random password generator, or token based PKI)	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.3(i)	i)Enforce two-factor authentication process for remote access (e.g., PIN based token card with a one-time random password generator, or token based PKI)	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
3.1.3(i)	i)Enforce two-factor authentication process for remote access (e.g., PIN based token card with a one-time random password generator, or token based PKI)	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
3.1.3(i)	i)Enforce two-factor authentication process for remote access (e.g., PIN based token card with a one-time random password generator, or token based PKI)	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.4(c)(e)	<p>c) The patch management process should include aspects like: - Determining methods of obtaining and validating patches for ensuring that the patch is from an authorised source - Identifying vulnerabilities that are applicable to applications and systems used by the organisation - Assessing the business impact of implementing patches (or not implementing a particular patch) - Ensuring patches are tested - Describing methods for deploying patches, e.g. automatically - Reporting on the status of patch deployment across the organisation and - Including methods for dealing with the failed deployment of a patch (e.g., redeployment of the patch). e) BFI should deploy automated patch management tools and software update tools for all systems for which such tools are available and safe</p>	<p><a href="#">ec2-instance-managed-by-systems-manager</a> (p. 132)</p>	<p>An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.4(c)(e)	<p>c) The patch management process should include aspects like: - Determining methods of obtaining and validating patches for ensuring that the patch is from an authorised source - Identifying vulnerabilities that are applicable to applications and systems used by the organisation - Assessing the business impact of implementing patches (or not implementing a particular patch) - Ensuring patches are tested - Describing methods for deploying patches, e.g. automatically - Reporting on the status of patch deployment across the organisation and - Including methods for dealing with the failed deployment of a patch (e.g., redeployment of the patch). e) BFI should deploy automated patch management tools and software update tools for all systems for which such tools are available and safe</p>	<p><a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a></p>	<p>Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.4(c)(e)	<p>c) The patch management process should include aspects like: - Determining methods of obtaining and validating patches for ensuring that the patch is from an authorised source - Identifying vulnerabilities that are applicable to applications and systems used by the organisation - Assessing the business impact of implementing patches (or not implementing a particular patch) - Ensuring patches are tested - Describing methods for deploying patches, e.g. automatically - Reporting on the status of patch deployment across the organisation and - Including methods for dealing with the failed deployment of a patch (e.g., redeployment of the patch). e) BFI should deploy automated patch management tools and software update tools for all systems for which such tools are available and safe</p>	<p><a href="#">ec2-managedinstance-patch-compliance-status-check</a> (p. 136)</p>	<p>Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.5(d)(e)	<p>d) Appropriate key management requires secure processes for generating, storing, archiving, retrieving, distributing, retiring and destroying cryptographic keys e) All cryptographic keys should be protected against modification and loss. In addition, secret and private keys need protection against unauthorised use as well as disclosure. Equipment used to generate, store and archive keys should be physically protected</p>	<p><a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a></p>	<p>To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.</p>
3.1.5(d)(e)	<p>d) Appropriate key management requires secure processes for generating, storing, archiving, retrieving, distributing, retiring and destroying cryptographic keys e) All cryptographic keys should be protected against modification and loss. In addition, secret and private keys need protection against unauthorised use as well as disclosure. Equipment used to generate, store and archive keys should be physically protected</p>	<p><a href="#">cmk-backing-key-rotation-enabled (p. 123)</a></p>	<p>Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.5(f)	<p>f) A key management system should be based on an agreed set of standards, procedures and secure methods for:</p> <ul style="list-style-type: none"><li>- generating keys for different cryptographic systems and different applications</li><li>- issuing and obtaining public key certificates</li><li>- distributing keys to intended entities, including how keys should be activated when received</li><li>- storing keys, including how authorised users obtain access to keys</li><li>- changing or updating keys including rules on when keys should be changed and how this will be done</li><li>- dealing with compromised keys</li><li>- revoking keys including how keys should be withdrawn or deactivated, e.g. when keys have been compromised or when a user leaves an organisation (in which case keys should also be archived)</li><li>- recovering keys that are lost or corrupted</li><li>- backing up or archiving keys</li><li>- destroying keys, and</li><li>- logging and auditing of key management related activities.</li></ul>	<p><a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a></p>	<p>To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.5(f)	<p>f) A key management system should be based on an agreed set of standards, procedures and secure methods for:</p> <ul style="list-style-type: none"><li>- generating keys for different cryptographic systems and different applications</li><li>- issuing and obtaining public key certificates</li><li>- distributing keys to intended entities, including how keys should be activated when received</li><li>- storing keys, including how authorised users obtain access to keys</li><li>- changing or updating keys including rules on when keys should be changed and how this will be done</li><li>- dealing with compromised keys</li><li>- revoking keys including how keys should be withdrawn or deactivated, e.g. when keys have been compromised or when a user leaves an organisation (in which case keys should also be archived)</li><li>- recovering keys that are lost or corrupted</li><li>- backing up or archiving keys</li><li>- destroying keys, and</li><li>- logging and auditing of key management related activities.</li></ul>	<p><a href="#">cmk-backing-key-rotation-enabled (p. 123)</a></p>	<p>Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.5(f)	<p>f) A key management system should be based on an agreed set of standards, procedures and secure methods for:</p> <ul style="list-style-type: none"><li>- generating keys for different cryptographic systems and different applications</li><li>- issuing and obtaining public key certificates</li><li>- distributing keys to intended entities, including how keys should be activated when received</li><li>- storing keys, including how authorised users obtain access to keys</li><li>- changing or updating keys including rules on when keys should be changed and how this will be done</li><li>- dealing with compromised keys</li><li>- revoking keys including how keys should be withdrawn or deactivated, e.g. when keys have been compromised or when a user leaves an organisation (in which case keys should also be archived)</li><li>- recovering keys that are lost or corrupted</li><li>- backing up or archiving keys</li><li>- destroying keys, and</li><li>- logging and auditing of key management related activities.</li></ul>	<p><a href="#">acm-certificate-expiration-check (p. 108)</a></p>	<p>Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.5(f)	<p>f) A key management system should be based on an agreed set of standards, procedures and secure methods for:</p> <ul style="list-style-type: none"><li>- generating keys for different cryptographic systems and different applications</li><li>- issuing and obtaining public key certificates</li><li>- distributing keys to intended entities, including how keys should be activated when received</li><li>- storing keys, including how authorised users obtain access to keys</li><li>- changing or updating keys including rules on when keys should be changed and how this will be done</li><li>- dealing with compromised keys</li><li>- revoking keys including how keys should be withdrawn or deactivated, e.g. when keys have been compromised or when a user leaves an organisation (in which case keys should also be archived)</li><li>- recovering keys that are lost or corrupted</li><li>- backing up or archiving keys</li><li>- destroying keys, and</li><li>- logging and auditing of key management related activities.</li></ul>	<a href="#">elb-acm-certificate-required (p. 143)</a>	<p>Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.5(f)	<p>f) A key management system should be based on an agreed set of standards, procedures and secure methods for:</p> <ul style="list-style-type: none"><li>- generating keys for different cryptographic systems and different applications</li><li>- issuing and obtaining public key certificates</li><li>- distributing keys to intended entities, including how keys should be activated when received</li><li>- storing keys, including how authorised users obtain access to keys</li><li>- changing or updating keys including rules on when keys should be changed and how this will be done</li><li>- dealing with compromised keys</li><li>- revoking keys including how keys should be withdrawn or deactivated, e.g. when keys have been compromised or when a user leaves an organisation (in which case keys should also be archived)</li><li>- recovering keys that are lost or corrupted</li><li>- backing up or archiving keys</li><li>- destroying keys, and</li><li>- logging and auditing of key management related activities.</li></ul>	<p><a href="#">cloudtrail-enabled (p. 121)</a></p>	<p>AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.5(f)	<p>f) A key management system should be based on an agreed set of standards, procedures and secure methods for:</p> <ul style="list-style-type: none"> <li>- generating keys for different cryptographic systems and different applications</li> <li>- issuing and obtaining public key certificates</li> <li>- distributing keys to intended entities, including how keys should be activated when received</li> <li>- storing keys, including how authorised users obtain access to keys</li> <li>- changing or updating keys including rules on when keys should be changed and how this will be done</li> <li>- dealing with compromised keys</li> <li>- revoking keys including how keys should be withdrawn or deactivated, e.g. when keys have been compromised or when a user leaves an organisation (in which case keys should also be archived)</li> <li>- recovering keys that are lost or corrupted</li> <li>- backing up or archiving keys</li> <li>- destroying keys, and</li> <li>- logging and auditing of key management related activities.</li> </ul>	<p><a href="#">multi-region-cloudtrail-enabled (p. 163)</a></p>	<p>AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.6(a)	a) The BFI should deploy a combination of automated tools and manual techniques to perform a comprehensive VA on a periodic basis. For web-based external facing systems, the scope of VA should include common web vulnerabilities such as SQL injection and cross-site scripting.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
3.1.6(a)	a) The BFI should deploy a combination of automated tools and manual techniques to perform a comprehensive VA on a periodic basis. For web-based external facing systems, the scope of VA should include common web vulnerabilities such as SQL injection and cross-site scripting.	<a href="#">alb-waf-enabled (p. 109)</a>	Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.
3.1.6(f)	f) The security function should provide status updates regarding the number of unmitigated, critical vulnerabilities, for each department/division, and plan for mitigating to senior management on a periodic basis	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.10(b)	b) Sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (e.g., integrity checkers, cryptographic hashes). Furthermore, policies should minimise the distribution of sensitive information, including printouts that contain the information.	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
3.1.10(b)	b) Sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (e.g., integrity checkers, cryptographic hashes). Furthermore, policies should minimise the distribution of sensitive information, including printouts that contain the information.	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
3.1.10(b)	b) Sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (e.g., integrity checkers, cryptographic hashes). Furthermore, policies should minimise the distribution of sensitive information, including printouts that contain the information.	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).

Control ID	Control Description	AWS Config Rule	Guidance
3.1.10(b)	b) Sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (e.g., integrity checkers, cryptographic hashes). Furthermore, policies should minimise the distribution of sensitive information, including printouts that contain the information.	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
3.1.10(b)	b) Sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (e.g., integrity checkers, cryptographic hashes). Furthermore, policies should minimise the distribution of sensitive information, including printouts that contain the information.	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
3.1.10(b)	b) Sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (e.g., integrity checkers, cryptographic hashes). Furthermore, policies should minimise the distribution of sensitive information, including printouts that contain the information.	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.10(b)	<p>b) Sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (e.g., integrity checkers, cryptographic hashes). Furthermore, policies should minimise the distribution of sensitive information, including printouts that contain the information.</p>	<p><a href="#">redshift-cluster-configuration-check (p. 170)</a></p>	<p>To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.</p>
3.1.10(b)	<p>b) Sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (e.g., integrity checkers, cryptographic hashes). Furthermore, policies should minimise the distribution of sensitive information, including printouts that contain the information.</p>	<p><a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a></p>	<p>To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1.10(b)	b) Sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (e.g., integrity checkers, cryptographic hashes). Furthermore, policies should minimise the distribution of sensitive information, including printouts that contain the information.	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.
3.1.10(b)	b) Sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (e.g., integrity checkers, cryptographic hashes). Furthermore, policies should minimise the distribution of sensitive information, including printouts that contain the information.	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.
3.1.10(b)	b) Sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (e.g., integrity checkers, cryptographic hashes). Furthermore, policies should minimise the distribution of sensitive information, including printouts that contain the information.	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.10(b)	b) Sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (e.g., integrity checkers, cryptographic hashes). Furthermore, policies should minimise the distribution of sensitive information, including printouts that contain the information.	<a href="#">ec2-ebs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
3.1.10(b)	b) Sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (e.g., integrity checkers, cryptographic hashes). Furthermore, policies should minimise the distribution of sensitive information, including printouts that contain the information.	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.
3.1.10(b)	b) Sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (e.g., integrity checkers, cryptographic hashes). Furthermore, policies should minimise the distribution of sensitive information, including printouts that contain the information.	<a href="#">s3-default-encryption-kms (p. 182)</a>	To help protect data at rest, ensure that encryption is enabled for your S3 buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. For more information about the encryption process and administration, use the AWS Key Management Service (AWS KMS) customer-managed CMKs.

Control ID	Control Description	AWS Config Rule	Guidance
3.2.1(h)	h) To minimise risks associated with changes, BFIs should perform backups of affected systems or applications prior to the change. BFIs should establish a rollback plan to revert to a former version of the system or application if a problem is encountered during or after the deployment.	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.
3.2.1(h)	h) To minimise risks associated with changes, BFIs should perform backups of affected systems or applications prior to the change. BFIs should establish a rollback plan to revert to a former version of the system or application if a problem is encountered during or after the deployment.	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.
3.2.1(h)	h) To minimise risks associated with changes, BFIs should perform backups of affected systems or applications prior to the change. BFIs should establish a rollback plan to revert to a former version of the system or application if a problem is encountered during or after the deployment.	<a href="#">ebs-optimized-instance (p. 131)</a>	An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance.

Control ID	Control Description	AWS Config Rule	Guidance
3.2.1(h)	h) To minimise risks associated with changes, BFIs should perform backups of affected systems or applications prior to the change. BFIs should establish a rollback plan to revert to a former version of the system or application if a problem is encountered during or after the deployment.	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
3.2.1(h)	h) To minimise risks associated with changes, BFIs should perform backups of affected systems or applications prior to the change. BFIs should establish a rollback plan to revert to a former version of the system or application if a problem is encountered during or after the deployment.	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
3.2.1(h)	h) To minimise risks associated with changes, BFIs should perform backups of affected systems or applications prior to the change. BFIs should establish a rollback plan to revert to a former version of the system or application if a problem is encountered during or after the deployment.	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.

Control ID	Control Description	AWS Config Rule	Guidance
3.2.1(h)	h) To minimise risks associated with changes, BFIs should perform backups of affected systems or applications prior to the change. BFIs should establish a rollback plan to revert to a former version of the system or application if a problem is encountered during or after the deployment.	<a href="#">dynamodb-in-backup-plan (p. 128)</a>	To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
3.2.1(h)	h) To minimise risks associated with changes, BFIs should perform backups of affected systems or applications prior to the change. BFIs should establish a rollback plan to revert to a former version of the system or application if a problem is encountered during or after the deployment.	<a href="#">ebs-in-backup-plan (p. 130)</a>	To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
3.2.1(h)	h) To minimise risks associated with changes, BFIs should perform backups of affected systems or applications prior to the change. BFIs should establish a rollback plan to revert to a former version of the system or application if a problem is encountered during or after the deployment.	<a href="#">efs-in-backup-plan (p. 139)</a>	To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	Control Description	AWS Config Rule	Guidance
3.2.1(h)	h) To minimise risks associated with changes, BFIs should perform backups of affected systems or applications prior to the change. BFIs should establish a rollback plan to revert to a former version of the system or application if a problem is encountered during or after the deployment.	<a href="#">rds-in-backup-plan (p. 167)</a>	To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
3.2.1(k)	k) Audit and security logs are useful information which facilitates investigations and trouble shooting. The BFI should ensure that the logging facility is enabled to record activities that are performed during the migration process.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
3.2.1(k)	k) Audit and security logs are useful information which facilitates investigations and trouble shooting. The BFI should ensure that the logging facility is enabled to record activities that are performed during the migration process.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
3.2.1(k)	k) Audit and security logs are useful information which facilitates investigations and trouble shooting. The BFI should ensure that the logging facility is enabled to record activities that are performed during the migration process.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
3.2.1(k)	k) Audit and security logs are useful information which facilitates investigations and trouble shooting. The BFI should ensure that the logging facility is enabled to record activities that are performed during the migration process.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
3.2.1(k)	k) Audit and security logs are useful information which facilitates investigations and trouble shooting. The BFI should ensure that the logging facility is enabled to record activities that are performed during the migration process.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
3.2.1(k)	k) Audit and security logs are useful information which facilitates investigations and trouble shooting. The BFI should ensure that the logging facility is enabled to record activities that are performed during the migration process.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
3.2.1(k)	k) Audit and security logs are useful information which facilitates investigations and trouble shooting. The BFI should ensure that the logging facility is enabled to record activities that are performed during the migration process.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
3.2.1(k)	k) Audit and security logs are useful information which facilitates investigations and trouble shooting. The BFI should ensure that the logging facility is enabled to record activities that are performed during the migration process.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
3.2.1(k)	k) Audit and security logs are useful information which facilitates investigations and trouble shooting. The BFI should ensure that the logging facility is enabled to record activities that are performed during the migration process.	<a href="#">cw-loggroup-retention-period-check (p. 125)</a>	Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events.
3.2.1(k)	k) Audit and security logs are useful information which facilitates investigations and trouble shooting. The BFI should ensure that the logging facility is enabled to record activities that are performed during the migration process.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.

Control ID	Control Description	AWS Config Rule	Guidance
3.2.1(k)	k) Audit and security logs are useful information which facilitates investigations and trouble shooting. The BFI should ensure that the logging facility is enabled to record activities that are performed during the migration process.	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.
3.2.1(k)	k) Audit and security logs are useful information which facilitates investigations and trouble shooting. The BFI should ensure that the logging facility is enabled to record activities that are performed during the migration process.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
3.3.2(a)	<p>a) The key aspects that are required to be considered include:</p> <ul style="list-style-type: none"> <li>- Completeness—ensuring that the total number of records from the source database is transferred to the new database (assuming the number of fields is the same).</li> <li>- Availability of data backup—ensuring that data is backed up before migration for future reference or any emergency that might arise out of the data migration process.</li> <li>- Integrity of data—ensuring that the data is not altered manually or electronically during the migration process. If such a need exists, having a documented plan to validate pre and post values for the changed data set should exist.</li> <li>- Consistency of data—the field/record called for from the new application should be consistent with that of the original application and</li> <li>- Continuity—the new application should be able to continue with newer records (or appendage) and help in ensuring seamless business continuity</li> </ul>	<p><a href="#">db-instance-backup-enabled (p. 126)</a></p>	<p>The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.2.2(a)	<p>a) The key aspects that are required to be considered include:</p> <ul style="list-style-type: none"><li>- Completeness—ensuring that the total number of records from the source database is transferred to the new database (assuming the number of fields is the same).</li><li>- Availability of data backup—ensuring that data is backed up before migration for future reference or any emergency that might arise out of the data migration process.</li><li>- Integrity of data—ensuring that the data is not altered manually or electronically during the migration process. If such a need exists, having a documented plan to validate pre and post values for the changed data set should exist.</li><li>- Consistency of data—the field/record called for from the new application should be consistent with that of the original application and</li><li>- Continuity—the new application should be able to continue with newer records (or appendage) and help in ensuring seamless business continuity</li></ul>	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	<p>Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.2.2(a)	<p>a) The key aspects that are required to be considered include:</p> <ul style="list-style-type: none"> <li>- Completeness—ensuring that the total number of records from the source database is transferred to the new database (assuming the number of fields is the same).</li> <li>- Availability of data backup—ensuring that data is backed up before migration for future reference or any emergency that might arise out of the data migration process.</li> <li>- Integrity of data—ensuring that the data is not altered manually or electronically during the migration process. If such a need exists, having a documented plan to validate pre and post values for the changed data set should exist.</li> <li>- Consistency of data—the field/record called for from the new application should be consistent with that of the original application and</li> <li>- Continuity—the new application should be able to continue with newer records (or appendage) and help in ensuring seamless business continuity</li> </ul>	<a href="#">ebs-optimized-instance (p. 131)</a>	<p>An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.2.2(a)	<p>a) The key aspects that are required to be considered include:</p> <ul style="list-style-type: none"> <li>- Completeness—ensuring that the total number of records from the source database is transferred to the new database (assuming the number of fields is the same).</li> <li>- Availability of data backup—ensuring that data is backed up before migration for future reference or any emergency that might arise out of the data migration process.</li> <li>- Integrity of data—ensuring that the data is not altered manually or electronically during the migration process. If such a need exists, having a documented plan to validate pre and post values for the changed data set should exist.</li> <li>- Consistency of data—the field/record called for from the new application should be consistent with that of the original application and</li> <li>- Continuity—the new application should be able to continue with newer records (or appendage) and help in ensuring seamless business continuity</li> </ul>	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	<p>When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.2.2(a)	<p>a) The key aspects that are required to be considered include:</p> <ul style="list-style-type: none"><li>- Completeness—ensuring that the total number of records from the source database is transferred to the new database (assuming the number of fields is the same).</li><li>- Availability of data backup—ensuring that data is backed up before migration for future reference or any emergency that might arise out of the data migration process.</li><li>- Integrity of data—ensuring that the data is not altered manually or electronically during the migration process. If such a need exists, having a documented plan to validate pre and post values for the changed data set should exist.</li><li>- Consistency of data—the field/record called for from the new application should be consistent with that of the original application and</li><li>- Continuity—the new application should be able to continue with newer records (or appendage) and help in ensuring seamless business continuity</li></ul>	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	<p>Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.2.2(a)	<p>a) The key aspects that are required to be considered include:</p> <ul style="list-style-type: none"><li>- Completeness—ensuring that the total number of records from the source database is transferred to the new database (assuming the number of fields is the same).</li><li>- Availability of data backup—ensuring that data is backed up before migration for future reference or any emergency that might arise out of the data migration process.</li><li>- Integrity of data—ensuring that the data is not altered manually or electronically during the migration process. If such a need exists, having a documented plan to validate pre and post values for the changed data set should exist.</li><li>- Consistency of data—the field/record called for from the new application should be consistent with that of the original application and</li><li>- Continuity—the new application should be able to continue with newer records (or appendage) and help in ensuring seamless business continuity</li></ul>	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	<p>Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.2.2(a)	<p>a) The key aspects that are required to be considered include:</p> <ul style="list-style-type: none"> <li>- Completeness—ensuring that the total number of records from the source database is transferred to the new database (assuming the number of fields is the same).</li> <li>- Availability of data backup—ensuring that data is backed up before migration for future reference or any emergency that might arise out of the data migration process.</li> <li>- Integrity of data—ensuring that the data is not altered manually or electronically during the migration process. If such a need exists, having a documented plan to validate pre and post values for the changed data set should exist.</li> <li>- Consistency of data—the field/record called for from the new application should be consistent with that of the original application and</li> <li>- Continuity—the new application should be able to continue with newer records (or appendage) and help in ensuring seamless business continuity</li> </ul>	<a href="#">dynamodb-in-backup-plan (p. 128)</a>	<p>To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.2.2(a)	<p>a) The key aspects that are required to be considered include:</p> <ul style="list-style-type: none"> <li>- Completeness—ensuring that the total number of records from the source database is transferred to the new database (assuming the number of fields is the same).</li> <li>- Availability of data backup—ensuring that data is backed up before migration for future reference or any emergency that might arise out of the data migration process.</li> <li>- Integrity of data—ensuring that the data is not altered manually or electronically during the migration process. If such a need exists, having a documented plan to validate pre and post values for the changed data set should exist.</li> <li>- Consistency of data—the field/record called for from the new application should be consistent with that of the original application and</li> <li>- Continuity—the new application should be able to continue with newer records (or appendage) and help in ensuring seamless business continuity</li> </ul>	<a href="#">ebs-in-backup-plan (p. 130)</a>	<p>To help with data backup processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.2.2(a)	<p>a) The key aspects that are required to be considered include:</p> <ul style="list-style-type: none"> <li>- Completeness—ensuring that the total number of records from the source database is transferred to the new database (assuming the number of fields is the same).</li> <li>- Availability of data backup—ensuring that data is backed up before migration for future reference or any emergency that might arise out of the data migration process.</li> <li>- Integrity of data—ensuring that the data is not altered manually or electronically during the migration process. If such a need exists, having a documented plan to validate pre and post values for the changed data set should exist.</li> <li>- Consistency of data—the field/record called for from the new application should be consistent with that of the original application and</li> <li>- Continuity—the new application should be able to continue with newer records (or appendage) and help in ensuring seamless business continuity</li> </ul>	<a href="#">efs-in-backup-plan (p. 139)</a>	<p>To help with data backup processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.2.2(a)	<p>a) The key aspects that are required to be considered include:</p> <ul style="list-style-type: none"> <li>- Completeness—ensuring that the total number of records from the source database is transferred to the new database (assuming the number of fields is the same).</li> <li>- Availability of data backup—ensuring that data is backed up before migration for future reference or any emergency that might arise out of the data migration process.</li> <li>- Integrity of data—ensuring that the data is not altered manually or electronically during the migration process. If such a need exists, having a documented plan to validate pre and post values for the changed data set should exist.</li> <li>- Consistency of data—the field/record called for from the new application should be consistent with that of the original application and</li> <li>- Continuity—the new application should be able to continue with newer records (or appendage) and help in ensuring seamless business continuity</li> </ul>	<a href="#">rds-in-backup-plan (p. 167)</a>	<p>To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.2.2(a)	a) Develop and implement processes for preventing, detecting, analysing and responding to information security incidents.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
3.2.2(a)	a) Develop and implement processes for preventing, detecting, analysing and responding to information security incidents.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
3.3.1(a)	a) Consider important factors associated with maintaining high system availability, adequate capacity, reliable performance, fast response time, scalability as part of the system design.	<a href="#">dynamodb-autoscaling-enabled (p. 128)</a>	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.

Control ID	Control Description	AWS Config Rule	Guidance
3.3.1(a)	a) Consider important factors associated with maintaining high system availability, adequate capacity, reliable performance, fast response time, scalability as part of the system design.	<a href="#">ebs-optimized-instance (p. 131)</a>	An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance.
3.3.1(a)	a) Consider important factors associated with maintaining high system availability, adequate capacity, reliable performance, fast response time, scalability as part of the system design.	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.

Control ID	Control Description	AWS Config Rule	Guidance
3.3.1(a)	a) Consider important factors associated with maintaining high system availability, adequate capacity, reliable performance, fast response time, scalability as part of the system design.	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
3.3.1(a)	a) Consider important factors associated with maintaining high system availability, adequate capacity, reliable performance, fast response time, scalability as part of the system design.	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
3.3.1(a)	a) Consider important factors associated with maintaining high system availability, adequate capacity, reliable performance, fast response time, scalability as part of the system design.	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.
3.3.1(a)	a) Consider important factors associated with maintaining high system availability, adequate capacity, reliable performance, fast response time, scalability as part of the system design.	<a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a>	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.
3.3.1(a)	a) Consider important factors associated with maintaining high system availability, adequate capacity, reliable performance, fast response time, scalability as part of the system design.	<a href="#">rds-instance-deletion-protection-enabled (p. 166)</a>	Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.

Control ID	Control Description	AWS Config Rule	Guidance
3.3.1(a)	a) Consider important factors associated with maintaining high system availability, adequate capacity, reliable performance, fast response time, scalability as part of the system design.	<a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a>	The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.
3.3.1(a)	a) Consider important factors associated with maintaining high system availability, adequate capacity, reliable performance, fast response time, scalability as part of the system design.	<a href="#">dynamodb-throughput-limit-check (p. 130)</a>	Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set <code>accountRCUThresholdPercentage</code> (Config Default: 80) and <code>accountWCUThresholdPercentage</code> (Config Default: 80) parameters. The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
3.3.1(a)	a) Consider important factors associated with maintaining high system availability, adequate capacity, reliable performance, fast response time, scalability as part of the system design.	<a href="#">lambda-concurrency-check (p. 161)</a>	This rule ensures that a Lambda function's concurrency high and low limits are established. This can assist in baselining the number of requests that your function is serving at any given time.
3.3.1(f)	f) Install appropriate mechanisms to backup data to meet the RTO- Recovery Time Objective and RPO- Recovery Point Objective requirements as identified through the risk assessment process.	<a href="#">dynamodb-in-backup-plan (p. 128)</a>	To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
3.3.1(f)	f) Install appropriate mechanisms to backup data to meet the RTO- Recovery Time Objective and RPO- Recovery Point Objective requirements as identified through the risk assessment process.	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.

Control ID	Control Description	AWS Config Rule	Guidance
3.3.1(f)	f) Install appropriate mechanisms to backup data to meet the RTO- Recovery Time Objective and RPO- Recovery Point Objective requirements as identified through the risk assessment process.	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
3.3.1(f)	f) Install appropriate mechanisms to backup data to meet the RTO- Recovery Time Objective and RPO- Recovery Point Objective requirements as identified through the risk assessment process.	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.
3.3.1(f)	f) Install appropriate mechanisms to backup data to meet the RTO- Recovery Time Objective and RPO- Recovery Point Objective requirements as identified through the risk assessment process.	<a href="#">ebs-in-backup-plan (p. 130)</a>	To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	Control Description	AWS Config Rule	Guidance
3.3.1(f)	f) Install appropriate mechanisms to backup data to meet the RTO- Recovery Time Objective and RPO- Recovery Point Objective requirements as identified through the risk assessment process.	<a href="#">efs-in-backup-plan (p. 139)</a>	To help with data backup processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
3.3.1(f)	f) Install appropriate mechanisms to backup data to meet the RTO- Recovery Time Objective and RPO- Recovery Point Objective requirements as identified through the risk assessment process.	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.
3.3.1(f)	f) Install appropriate mechanisms to backup data to meet the RTO- Recovery Time Objective and RPO- Recovery Point Objective requirements as identified through the risk assessment process.	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.

Control ID	Control Description	AWS Config Rule	Guidance
3.3.1(f)	f) Install appropriate mechanisms to backup data to meet the RTO- Recovery Time Objective and RPO- Recovery Point Objective requirements as identified through the risk assessment process.	<a href="#">rds-in-backup-plan (p. 167)</a>	To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
3.4(a)(b)(c)(f)(j)	a) Ensure that records of user access are uniquely identified and logged for audit and review purposes. b) Have accountability and identification of unauthorised access is documented. c) Enable audit logging of system activities performed by privileged users. f) Ensure appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security. j) Ensure event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.

Control ID	Control Description	AWS Config Rule	Guidance
3.4(a)(b)(c)(f)(j)	<p>a) Ensure that records of user access are uniquely identified and logged for audit and review purposes. b) Have accountability and identification of unauthorised access is documented. c) Enable audit logging of system activities performed by privileged users. f) Ensure appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security. j) Ensure event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security.</p>	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	<p>Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.4(a)(b)(c)(f)(j)	<p>a) Ensure that records of user access are uniquely identified and logged for audit and review purposes. b) Have accountability and identification of unauthorised access is documented. c) Enable audit logging of system activities performed by privileged users. f) Ensure appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security. j) Ensure event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security.</p>	<a href="#">cloudtrail-enabled (p. 121)</a>	<p>AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.4(a)(b)(c)(f)(j)	<p>a) Ensure that records of user access are uniquely identified and logged for audit and review purposes. b) Have accountability and identification of unauthorised access is documented. c) Enable audit logging of system activities performed by privileged users. f) Ensure appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security. j) Ensure event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security.</p>	<p><a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a></p>	<p>The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.4(a)(b)(c)(f)(j)	<p>a) Ensure that records of user access are uniquely identified and logged for audit and review purposes. b) Have accountability and identification of unauthorised access is documented. c) Enable audit logging of system activities performed by privileged users. f) Ensure appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security. j) Ensure event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security.</p>	<a href="#">elb-logging-enabled (p. 144)</a>	<p>Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.4(a)(b)(c)(f)(j)	<p>a) Ensure that records of user access are uniquely identified and logged for audit and review purposes. b) Have accountability and identification of unauthorised access is documented. c) Enable audit logging of system activities performed by privileged users. f) Ensure appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security. j) Ensure event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security.</p>	<p><a href="#">multi-region-cloudtrail-enabled (p. 163)</a></p>	<p>AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.4(a)(b)(c)(f)(j)	<p>a) Ensure that records of user access are uniquely identified and logged for audit and review purposes. b) Have accountability and identification of unauthorised access is documented. c) Enable audit logging of system activities performed by privileged users. f) Ensure appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security. j) Ensure event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security.</p>	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	<p>Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.4(a)(b)(c)(f)(j)	<p>a) Ensure that records of user access are uniquely identified and logged for audit and review purposes. b) Have accountability and identification of unauthorised access is documented. c) Enable audit logging of system activities performed by privileged users. f) Ensure appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security. j) Ensure event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security.</p>	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	<p>The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.4(a)(b)(c)(f)(j)	<p>a) Ensure that records of user access are uniquely identified and logged for audit and review purposes. b) Have accountability and identification of unauthorised access is documented. c) Enable audit logging of system activities performed by privileged users. f) Ensure appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security. j) Ensure event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security.</p>	<a href="#">rds-logging-enabled (p. 167)</a>	<p>To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.4(a)(b)(c)(f)(j)	<p>a) Ensure that records of user access are uniquely identified and logged for audit and review purposes. b) Have accountability and identification of unauthorised access is documented. c) Enable audit logging of system activities performed by privileged users. f) Ensure appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security. j) Ensure event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security.</p>	<a href="#">wafv2-logging-enabled (p. 190)</a>	<p>To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.4(a)(b)(c)(f)(j)	<p>a) Ensure that records of user access are uniquely identified and logged for audit and review purposes. b) Have accountability and identification of unauthorised access is documented. c) Enable audit logging of system activities performed by privileged users. f) Ensure appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security. j) Ensure event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security.</p>	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	<p>To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.4(g)	<p>g) Ensure event logs include, when relevant:</p> <ul style="list-style-type: none"><li>- User IDs - System activities - Dates, time and details of key events, e.g. log-on and log-off - Device identity or location if possible and system identifier - Records of successful and rejected system access attempts</li><li>- Records of successful and rejected data and other resource access attempts - Changes to system configuration</li><li>- Use of privileges - Use of system utilities and applications - Files accessed and the kind of access - Network addresses and protocols</li><li>- Alarms raised by the access control system and - Records of transactions executed by users in applications and online customer transaction</li></ul>	<a href="#">cloudtrail-enabled (p. 121)</a>	<p>AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.4(g)	<p>g) Ensure event logs include, when relevant:</p> <ul style="list-style-type: none"><li>- User IDs - System activities - Dates, time and details of key events, e.g. log-on and log-off - Device identity or location if possible and system identifier - Records of successful and rejected system access attempts</li><li>- Records of successful and rejected data and other resource access attempts - Changes to system configuration</li><li>- Use of privileges - Use of system utilities and applications - Files accessed and the kind of access - Network addresses and protocols</li><li>- Alarms raised by the access control system and - Records of transactions executed by users in applications and online customer transaction</li></ul>	<p><a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a></p>	<p>The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.4(g)	<p>g) Ensure event logs include, when relevant:</p> <ul style="list-style-type: none"><li>- User IDs - System activities - Dates, time and details of key events, e.g. log-on and log-off - Device identity or location if possible and system identifier - Records of successful and rejected system access attempts</li><li>- Records of successful and rejected data and other resource access attempts - Changes to system configuration</li><li>- Use of privileges - Use of system utilities and applications - Files accessed and the kind of access - Network addresses and protocols</li><li>- Alarms raised by the access control system and - Records of transactions executed by users in applications and online customer transaction</li></ul>	<p><a href="#">api-gw-execution-logging-enabled (p. 111)</a></p>	<p>API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.4(g)	<p>g) Ensure event logs include, when relevant:</p> <ul style="list-style-type: none"><li>- User IDs - System activities - Dates, time and details of key events, e.g. log-on and log-off - Device identity or location if possible and system identifier - Records of successful and rejected system access attempts</li><li>- Records of successful and rejected data and other resource access attempts - Changes to system configuration</li><li>- Use of privileges - Use of system utilities and applications - Files accessed and the kind of access - Network addresses and protocols</li><li>- Alarms raised by the access control system and - Records of transactions executed by users in applications and online customer transaction</li></ul>	<p><a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a></p>	<p>Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.4(g)	<p>g) Ensure event logs include, when relevant:</p> <ul style="list-style-type: none"><li>- User IDs - System activities - Dates, time and details of key events, e.g. log-on and log-off - Device identity or location if possible and system identifier - Records of successful and rejected system access attempts</li><li>- Records of successful and rejected data and other resource access attempts - Changes to system configuration</li><li>- Use of privileges - Use of system utilities and applications - Files accessed and the kind of access - Network addresses and protocols</li><li>- Alarms raised by the access control system and - Records of transactions executed by users in applications and online customer transaction</li></ul>	<p><a href="#">elb-logging-enabled (p. 144)</a></p>	<p>Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.4(g)	<p>g) Ensure event logs include, when relevant:</p> <ul style="list-style-type: none"><li>- User IDs - System activities - Dates, time and details of key events, e.g. log-on and log-off - Device identity or location if possible and system identifier - Records of successful and rejected system access attempts</li><li>- Records of successful and rejected data and other resource access attempts - Changes to system configuration</li><li>- Use of privileges - Use of system utilities and applications - Files accessed and the kind of access - Network addresses and protocols</li><li>- Alarms raised by the access control system and - Records of transactions executed by users in applications and online customer transaction</li></ul>	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	<p>AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.4(g)	<p>g) Ensure event logs include, when relevant:</p> <ul style="list-style-type: none"><li>- User IDs - System activities - Dates, time and details of key events, e.g. log-on and log-off - Device identity or location if possible and system identifier - Records of successful and rejected system access attempts</li><li>- Records of successful and rejected data and other resource access attempts - Changes to system configuration</li><li>- Use of privileges - Use of system utilities and applications - Files accessed and the kind of access - Network addresses and protocols</li><li>- Alarms raised by the access control system and - Records of transactions executed by users in applications and online customer transaction</li></ul>	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	<p>The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.4(g)	g) Ensure event logs include, when relevant: - User IDs - System activities - Dates, time and details of key events, e.g. log-on and log-off - Device identity or location if possible and system identifier - Records of successful and rejected system access attempts - Records of successful and rejected data and other resource access attempts - Changes to system configuration - Use of privileges - Use of system utilities and applications - Files accessed and the kind of access - Network addresses and protocols - Alarms raised by the access control system and - Records of transactions executed by users in applications and online customer transaction	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
3.4(g)	<p>g) Ensure event logs include, when relevant:</p> <ul style="list-style-type: none"><li>- User IDs - System activities - Dates, time and details of key events, e.g. log-on and log-off - Device identity or location if possible and system identifier - Records of successful and rejected system access attempts</li><li>- Records of successful and rejected data and other resource access attempts - Changes to system configuration</li><li>- Use of privileges - Use of system utilities and applications - Files accessed and the kind of access - Network addresses and protocols</li><li>- Alarms raised by the access control system and - Records of transactions executed by users in applications and online customer transaction</li></ul>	<p><a href="#">rds-logging-enabled (p. 167)</a></p>	<p>To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.4(g)	<p>g) Ensure event logs include, when relevant:</p> <ul style="list-style-type: none"><li>- User IDs - System activities - Dates, time and details of key events, e.g. log-on and log-off - Device identity or location if possible and system identifier - Records of successful and rejected system access attempts</li><li>- Records of successful and rejected data and other resource access attempts - Changes to system configuration</li><li>- Use of privileges - Use of system utilities and applications - Files accessed and the kind of access - Network addresses and protocols</li><li>- Alarms raised by the access control system and - Records of transactions executed by users in applications and online customer transaction</li></ul>	<p><a href="#">redshift-cluster-configuration-check (p. 170)</a></p>	<p>To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.4(g)	<p>g) Ensure event logs include, when relevant:</p> <ul style="list-style-type: none"> <li>- User IDs - System activities - Dates, time and details of key events, e.g. log-on and log-off - Device identity or location if possible and system identifier - Records of successful and rejected system access attempts</li> <li>- Records of successful and rejected data and other resource access attempts - Changes to system configuration</li> <li>- Use of privileges - Use of system utilities and applications - Files accessed and the kind of access - Network addresses and protocols</li> <li>- Alarms raised by the access control system and - Records of transactions executed by users in applications and online customer transaction</li> </ul>	<p><a href="#">wafv2-logging-enabled (p. 190)</a></p>	<p>To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.</p>
3.6.1(a)(h)	<p>a) BFIs need to ensure suitable security measures for their web applications and take reasonable mitigating measures against various web security risks. h) BFIs need to ensure suitable security measures for their web applications and take reasonable mitigating measures against various web security risks</p>	<p><a href="#">alb-waf-enabled (p. 109)</a></p>	<p>Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.6.1(b)	b) BFIs need to evaluate security requirements associated with their internet banking systems and other relevant systems and adopt an encryption solution considering the degree of confidentiality and integrity required.	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.
3.6.1(b)	b) BFIs need to evaluate security requirements associated with their internet banking systems and other relevant systems and adopt an encryption solution considering the degree of confidentiality and integrity required.	<a href="#">alb-http-to-https-redirection-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
3.6.1(b)	b) BFIs need to evaluate security requirements associated with their internet banking systems and other relevant systems and adopt an encryption solution considering the degree of confidentiality and integrity required.	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
3.6.1(b)	b) BFIs need to evaluate security requirements associated with their internet banking systems and other relevant systems and adopt an encryption solution considering the degree of confidentiality and integrity required.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
3.6.1(b)	b) BFIs need to evaluate security requirements associated with their internet banking systems and other relevant systems and adopt an encryption solution considering the degree of confidentiality and integrity required.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
3.6.1(b)	b) BFIs need to evaluate security requirements associated with their internet banking systems and other relevant systems and adopt an encryption solution considering the degree of confidentiality and integrity required.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
3.6.1(b)	b) BFIs need to evaluate security requirements associated with their internet banking systems and other relevant systems and adopt an encryption solution considering the degree of confidentiality and integrity required.	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
3.6.1(b)	b) BFIs need to evaluate security requirements associated with their internet banking systems and other relevant systems and adopt an encryption solution considering the degree of confidentiality and integrity required.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
3.6.1(d)	d) BFIs providing internet banking should be responsive to unusual network traffic conditions/system performance and sudden surge in system resource utilisation which could be an indication of a DDoS attack. Consequently, the success of any pre-emptive and reactive actions depends on the deployment of appropriate tools to effectively detect, monitor and analyse anomalies in networks and systems.	<a href="#">alb-waf-enabled (p. 109)</a>	Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.
3.6.1(d)	d) BFIs providing internet banking should be responsive to unusual network traffic conditions/system performance and sudden surge in system resource utilisation which could be an indication of a DDoS attack. Consequently, the success of any pre-emptive and reactive actions depends on the deployment of appropriate tools to effectively detect, monitor and analyse anomalies in networks and systems.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
3.6.1(d)	d) BFIs providing internet banking should be responsive to unusual network traffic conditions/system performance and sudden surge in system resource utilisation which could be an indication of a DDoS attack. Consequently, the success of any pre-emptive and reactive actions depends on the deployment of appropriate tools to effectively detect, monitor and analyse anomalies in networks and systems.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
3.6.1(d)	d) BFIs providing internet banking should be responsive to unusual network traffic conditions/system performance and sudden surge in system resource utilisation which could be an indication of a DDoS attack. Consequently, the success of any pre-emptive and reactive actions depends on the deployment of appropriate tools to effectively detect, monitor and analyse anomalies in networks and systems.	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.

Control ID	Control Description	AWS Config Rule	Guidance
3.6.1(e)	e) BFIs need to regularly assess information security vulnerabilities and evaluate the effectiveness of the existing IT security risk management framework, making any necessary adjustments to ensure emerging vulnerabilities are addressed in a timely manner. This assessment should also be conducted as part of any material change.	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.
3.6.4(a)(b)	a) Restrict internet access and segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
3.6.4(a)(b)	a) Restrict internet access and segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
3.6.4(a)(b)	a) Restrict internet access and segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
3.6.4(a)(b)	a) Restrict internet access and segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
3.6.4(a)(b)	a) Restrict internet access and segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
3.6.4(a)(b)	a) Restrict internet access and segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
3.6.4(a)(b)	a) Restrict internet access and segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
3.6.4(a)(b)	a) Restrict internet access and segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
3.6.4(a)(b)	a) Restrict internet access and segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
3.6.4(a)(b)	a) Restrict internet access and segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
3.6.4(a)(b)	a) Restrict internet access and segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
3.6.4(a)(b)	a) Restrict internet access and segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
3.6.4(a)(b)	a) Restrict internet access and segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
3.6.4(a)(b)	a) Restrict internet access and segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
3.6.4(a)(b)	a) Restrict internet access and segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
3.6.4(a)(b)	a) Restrict internet access and segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
3.6.4(a)(b)	a) Restrict internet access and segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
3.6.4(a)(b)	a) Restrict internet access and segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
3.6.4(a)(b)	a) Restrict internet access and segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
3.6.4(a)(b)	a) Restrict internet access and segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.

## Template

The template is available on GitHub: [Operational Best Practices for NBC TRMG](#).

## Operational Best Practices for NERC CIP

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the North American Electric Reliability Corporation Critical Infrastructure Protection Standards (NERC CIP) AWS managed Config rules. Each AWS Config rule applies to a specific AWS resource, and relates to one or more NERC CIP controls. A NERC CIP control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

Control ID	Control Description	AWS Config Rule	Guidance
CIP-003-7-R2-Part 4	Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include: 4.1 Identification, classification, and response to Cyber Security Incidents; 4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law; 4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals; 4.4 Incident handling for Cyber Security Incidents; 4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by:	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
	(1) responding to an actual Reportable Cyber Security		
CIP-003-7-R2-Part 4	<p>Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:</p> <p>4.1 Identification, classification, and response to Cyber Security Incidents;</p> <p>4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;</p> <p>4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;</p> <p>4.4 Incident handling for Cyber Security Incidents;</p> <p>4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by:</p> <p>(1) responding to an actual Reportable Cyber Security</p>	<p><a href="#">guardduty-enabled-centralized (p. 152)</a></p>	<p>Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.</p>

Control ID	Control Description	AWS Config Rule	Guidance
CIP-003-8-Attachment 1-Section 3.1	Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to: 3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are: ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s).	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
CIP-003-8-Attachment 1-Section 3.1	Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to: 3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are: ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s).	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-003-8-Attachment 1-Section 3.1	Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to: 3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are: ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s).	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
CIP-003-8-Attachment 1-Section 3.1	Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to: 3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are: ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s).	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-003-8-Attachment 1-Section 3.1	Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to: 3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are: ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s).	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
CIP-003-8-Attachment 1-Section 3.1	Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to: 3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are: ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s).	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-003-8-Attachment 1-Section 3.1	<p>Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to: 3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are: ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s).</p>	<p><a href="#">ec2-instances-in-vpc (p. 159)</a></p>	<p>Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.</p>
CIP-003-8-Attachment 1-Section 3.1	<p>Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to: 3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are: ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s).</p>	<p><a href="#">internet-gateway-authorized-vpc-only (p. 160)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.</p>

Control ID	Control Description	AWS Config Rule	Guidance
CIP-003-8-Attachment 1-Section 3.1	Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to: 3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are: ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s).	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
CIP-003-8-Attachment 1-Section 3.1	Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to: 3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are: ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s).	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-003-8-Attachment 1-Section 3.1	Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to: 3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are: ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s).	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
CIP-003-8-Attachment 1-Section 3.1	Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to: 3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are: ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s).	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-003-8-Attachment 1-Section 3.1	Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to: 3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are: ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s).	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
CIP-003-8-Attachment 1-Section 3.1	Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to: 3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are: ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s).	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-003-8-Attachment 1-Section 3.1	<p>Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to: 3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are: ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s).</p>	<p><a href="#">s3-account-level-public-access-blocks (p. 175)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.</p>
CIP-003-8-Attachment 1-Section 3.1	<p>Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to: 3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are: ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s).</p>	<p><a href="#">s3-bucket-public-read-prohibited (p. 179)</a></p>	<p>Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
CIP-003-8-Attachment 1-Section 3.1	<p>Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to: 3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are: ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s).</p>	<p><a href="#">s3-bucket-public-write-prohibited (p. 180)</a></p>	<p>Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.</p>
CIP-003-8-Attachment 1-Section 3.1	<p>Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to: 3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are: ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s).</p>	<p><a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.</p>

Control ID	Control Description	AWS Config Rule	Guidance
CIP-003-8-Attachment 1-Section 3.1	<p>Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to: 3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are: ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s).</p>	<p><a href="#">vpc-default-security-group-closed (p. 188)</a></p>	<p>Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.</p>
CIP-003-8-Attachment 1-Section 3.1	<p>Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to: 3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are: ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s).</p>	<p><a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.</p>

Control ID	Control Description	AWS Config Rule	Guidance
CIP-004-6-R4-Part 4.1.1	Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program. 4.1.1. Electronic access.	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
CIP-004-6-R4-Part 4.1.1	Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program. 4.1.1. Electronic access.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-004-6-R4-Part 4.1.1	Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program. 4.1.1. Electronic access.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
CIP-004-6-R4-Part 4.1.1	Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program. 4.1.1. Electronic access.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
CIP-004-6-R4-Part 4.1.1	Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program. 4.1.1. Electronic access.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-004-6-R4-Part 4.1.1	Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program. 4.1.1. Electronic access.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
CIP-004-6-R4-Part 4.1.1	Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program. 4.1.1. Electronic access.	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.
CIP-004-6-R4-Part 4.1.1	Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program. 4.1.1. Electronic access.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-004-6-R4-Part 4.1.1	Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program. 4.1.1. Electronic access.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
CIP-004-6-R4-Part 4.1.1	Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program. 4.1.1. Electronic access.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
CIP-004-6-R4-Part 4.1.1	Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program. 4.1.1. Electronic access.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
CIP-004-6-R4-Part 4.1.1	Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program. 4.1.1. Electronic access.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-004-6-R4-Part 4.1.1	Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program. 4.1.1. Electronic access.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
CIP-004-6-R4-Part 4.1.1	Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program. 4.1.1. Electronic access.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
CIP-004-6-R4-Part 4.1.1	Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program. 4.1.1. Electronic access.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-004-6-R4-Part 4.1.1	Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program. 4.1.1. Electronic access.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
CIP-004-6-R4-Part 4.1.1	Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program. 4.1.1. Electronic access.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
CIP-004-6-R4-Part 4.1.3	Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program. 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-004-6-R4-Part 4.1.3	Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program. 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
CIP-004-6-R4-Part 4.1.3	Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program. 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
CIP-005-5-R1-Part 1.1	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. Part 1.1: All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-005-5-R1-Part 1.1	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. Part 1.1: All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
CIP-005-5-R1-Part 1.1	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. Part 1.1: All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
CIP-005-5-R1-Part 1.1	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. Part 1.1: All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-005-5-R1-Part 1.1	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. Part 1.1: All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
CIP-005-5-R1-Part 1.1	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. Part 1.1: All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-005-5-R1-Part 1.1	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. Part 1.1: All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
CIP-005-5-R1-Part 1.1	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. Part 1.1: All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-005-5-R1-Part 1.1	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. Part 1.1: All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
CIP-005-5-R1-Part 1.1	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. Part 1.1: All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-005-5-R1-Part 1.1	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. Part 1.1: All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
CIP-005-5-R1-Part 1.1	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. Part 1.1: All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-005-5-R1-Part 1.1	<p>Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. Part 1.1: All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.</p>	<p><a href="#">s3-account-level-public-access-blocks (p. 175)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.</p>
CIP-005-5-R1-Part 1.1	<p>Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. Part 1.1: All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.</p>	<p><a href="#">s3-bucket-public-read-prohibited (p. 179)</a></p>	<p>Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
CIP-005-5-R1-Part 1.1	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. Part 1.1: All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
CIP-005-5-R1-Part 1.1	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. Part 1.1: All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
CIP-005-5-R1-Part 1.2	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. Part 1.2: All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	<a href="#">alb-waf-enabled (p. 109)</a>	Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-005-5-R1-Part 1.2	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. Part 1.2: All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
CIP-005-5-R1-Part 1.3	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. Part 1.3: Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
CIP-005-5-R1-Part 1.3	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. Part 1.3: Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-005-5-R1-Part 1.3	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. Part 1.3: Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
CIP-005-5-R1-Part 1.3	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. Part 1.3: Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-005-5-R1-Part 1.3	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. Part 1.3: Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
CIP-005-5-R1-Part 1.3	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. Part 1.3: Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-005-5-R1-Part 1.3	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. Part 1.3: Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
CIP-005-5-R1-Part 1.3	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. Part 1.3: Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
CIP-005-5-R1-Part 1.3	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. Part 1.3: Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-005-5-R1-Part 1.3	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. Part 1.3: Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
CIP-005-5-R1-Part 1.3	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. Part 1.3: Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
CIP-005-5-R1-Part 1.3	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. Part 1.3: Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-005-5-R1-Part 1.3	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. Part 1.3: Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
CIP-005-5-R1-Part 1.5	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. Part 1.5: Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
CIP-005-5-R1-Part 1.5	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. Part 1.5: Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	<a href="#">alb-waf-enabled (p. 109)</a>	Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-005-5-R2-Part 2.2	Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-5 Table R2 – Interactive Remote Access Management. Part 2.2: For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
CIP-005-5-R2-Part 2.2	Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-5 Table R2 – Interactive Remote Access Management. Part 2.2: For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-005-5-R2-Part 2.2	Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-5 Table R2 – Interactive Remote Access Management. Part 2.2: For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
CIP-005-5-R2-Part 2.3	Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-5 Table R2 – Interactive Remote Access Management. Part 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-005-5-R2-Part 2.3	Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-5 Table R2 – Interactive Remote Access Management. Part 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
CIP-007-6-R1-Part 1.1	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R1 – Ports and Services. Part 1.1: Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-007-6-R1-Part 1.1	<p>Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R1 – Ports and Services. Part 1.1: Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.</p>	<p><a href="#">emr-master-no-public-ip (p. 146)</a></p>	<p>Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.</p>
CIP-007-6-R1-Part 1.1	<p>Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R1 – Ports and Services. Part 1.1: Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.</p>	<p><a href="#">restricted-ssh (p. 159)</a></p>	<p>Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.</p>

Control ID	Control Description	AWS Config Rule	Guidance
CIP-007-6-R1-Part 1.1	<p>Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R1 – Ports and Services. Part 1.1: Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.</p>	<p><a href="#">restricted-common-ports (p. 174)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.</p>
CIP-007-6-R1-Part 1.1	<p>Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R1 – Ports and Services. Part 1.1: Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.</p>	<p><a href="#">vpc-default-security-group-closed (p. 188)</a></p>	<p>Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.</p>

Control ID	Control Description	AWS Config Rule	Guidance
CIP-007-6-R1-Part 1.1	<p>Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R1 – Ports and Services. Part 1.1: Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.</p>	<p><a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.</p>
CIP-007-6-R2-Part 2.1	<p>Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R2 – Security Patch Management. Part 2.1: A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.</p>	<p><a href="#">guardduty-non-archived-findings (p. 152)</a></p>	<p>Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
CIP-007-6-R2-Part 2.1	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R2 – Security Patch Management. Part 2.1: A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-007-6-R2-Part 2.1	<p>Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R2 – Security Patch Management. Part 2.1: A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.</p>	<p><a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a></p>	<p>Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.</p>
CIP-007-6-R3-Part 3.1-2	<p>Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R2 – Security Patch Management. Part 3.1: Deploy method(s) to deter, detect, or prevent malicious code. Part 3.2: Mitigate the threat of detected malicious code.</p>	<p><a href="#">guardduty-enabled-centralized (p. 152)</a></p>	<p>Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.</p>

Control ID	Control Description	AWS Config Rule	Guidance
CIP-007-6-R3-Part 3.1-2	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R2 – Security Patch Management. Part 3.1: Deploy method(s) to deter, detect, or prevent malicious code. Part 3.2: Mitigate the threat of detected malicious code.	<a href="#">alb-waf-enabled (p. 109)</a>	Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.
CIP-007-6-R4-Part 4.1	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-007-6-R4-Part 4.1	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
CIP-007-6-R4-Part 4.1	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-007-6-R4-Part 4.1	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
CIP-007-6-R4-Part 4.1	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-007-6-R4-Part 4.1	<p>Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.</p>	<p><a href="#">multi-region-cloudtrail-enabled (p. 163)</a></p>	<p>AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.</p>
CIP-007-6-R4-Part 4.1	<p>Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.</p>	<p><a href="#">redshift-cluster-configuration-check (p. 170)</a></p>	<p>To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
CIP-007-6-R4-Part 4.1	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
CIP-007-6-R4-Part 4.1	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-007-6-R4-Part 4.1	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
CIP-007-6-R4-Part 4.1	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-007-6-R4-Part 4.3	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R4 – Security Event Monitoring. Part 4.3: Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	<a href="#">cw-loggroup-retention-period-check (p. 125)</a>	Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-007-6-R5-Part 5.1	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R5 – System Access Controls. Part 5.1: Have a method(s) to enforce authentication of interactive user access, where technically feasible.	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
CIP-008-5-R1-Part 1.1	Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include Part 1.1: One or more processes to identify, classify, and respond to Cyber Security Incidents.	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.
CIP-008-5-R1-Part 1.1	Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include Part 1.1: One or more processes to identify, classify, and respond to Cyber Security Incidents.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-008-5-R1-Part 1.1	Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include Part 1.1: One or more processes to identify, classify, and respond to Cyber Security Incidents.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
CIP-009-6-R1-Part 1.3	Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable requirement parts in CIP-009-6 Table R1 – Recovery Plan Specifications. Part 1.3: One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.
CIP-009-6-R1-Part 1.3	Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable requirement parts in CIP-009-6 Table R1 – Recovery Plan Specifications. Part 1.3: One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	<a href="#">dynamodb-in-backup-plan (p. 128)</a>	To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-009-6-R1-Part 1.3	Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable requirement parts in CIP-009-6 Table R1 – Recovery Plan Specifications. Part 1.3: One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.
CIP-009-6-R1-Part 1.3	Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable requirement parts in CIP-009-6 Table R1 – Recovery Plan Specifications. Part 1.3: One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	<a href="#">ebs-in-backup-plan (p. 130)</a>	To help with data backup processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
CIP-009-6-R1-Part 1.3	Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable requirement parts in CIP-009-6 Table R1 – Recovery Plan Specifications. Part 1.3: One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	<a href="#">efs-in-backup-plan (p. 139)</a>	To help with data backup processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-009-6-R1-Part 1.3	Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable requirement parts in CIP-009-6 Table R1 – Recovery Plan Specifications. Part 1.3: One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
CIP-009-6-R1-Part 1.3	Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable requirement parts in CIP-009-6 Table R1 – Recovery Plan Specifications. Part 1.3: One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	<a href="#">rds-in-backup-plan (p. 167)</a>	To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
CIP-009-6-R1-Part 1.3	Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable requirement parts in CIP-009-6 Table R1 – Recovery Plan Specifications. Part 1.3: One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-009-6-R1-Part 1.3	Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable requirement parts in CIP-009-6 Table R1 – Recovery Plan Specifications. Part 1.3: One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.
CIP-009-6-R1-Part 1.3	Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable requirement parts in CIP-009-6 Table R1 – Recovery Plan Specifications. Part 1.3: One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-010-2-R1-Part 1.1	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R1 – Configuration Change Management. Part 1.1: Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-010-2-R1-Part 1.1	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R1 – Configuration Change Management. Part 1.1: Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-010-2-R1-Part 1.1	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R1 – Configuration Change Management. Part 1.1: Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-010-2-R1-Part 1.1	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R1 – Configuration Change Management. Part 1.1: Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	<a href="#">ec2-stopped-instance (p. 137)</a>	Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-010-2-R1-Part 1.1	<p>Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R1 – Configuration Change Management. Part 1.1: Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.</p>	<p><a href="#">ec2-volume-inuse-check (p. 137)</a></p>	<p>This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality.</p>
CIP-011-2-R1-Part 1.2	<p>Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use. Part 1.2: Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.</p>	<p><a href="#">acm-certificate-expiration-check (p. 108)</a></p>	<p>Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
CIP-011-2-R1-Part 1.2	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use. Part 1.2: Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
CIP-011-2-R1-Part 1.2	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use. Part 1.2: Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
CIP-011-2-R1-Part 1.2	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use. Part 1.2: Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
CIP-011-2-R1-Part 1.2	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use. Part 1.2: Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-011-2-R1-Part 1.2	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use. Part 1.2: Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
CIP-011-2-R1-Part 1.2	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use. Part 1.2: Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	<a href="#">cmk-backing-key-rotation-enabled (p. 123)</a>	Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period.
CIP-011-2-R1-Part 1.2	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use. Part 1.2: Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	<a href="#">dynamodb-table-encrypted-kms (p. 129)</a>	Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK).
CIP-011-2-R1-Part 1.2	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use. Part 1.2: Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	<a href="#">ec2-ebs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-011-2-R1-Part 1.2	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use. Part 1.2: Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
CIP-011-2-R1-Part 1.2	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use. Part 1.2: Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
CIP-011-2-R1-Part 1.2	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use. Part 1.2: Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
CIP-011-2-R1-Part 1.2	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use. Part 1.2: Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-011-2-R1-Part 1.2	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use. Part 1.2: Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
CIP-011-2-R1-Part 1.2	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use. Part 1.2: Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
CIP-011-2-R1-Part 1.2	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use. Part 1.2: Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.
CIP-011-2-R1-Part 1.2	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use. Part 1.2: Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-011-2-R1-Part 1.2	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use. Part 1.2: Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.
CIP-011-2-R1-Part 1.2	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use. Part 1.2: Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.
CIP-011-2-R1-Part 1.2	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use. Part 1.2: Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-011-2-R1-Part 1.2	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use. Part 1.2: Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
CIP-011-2-R1-Part 1.2	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use. Part 1.2: Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
CIP-011-2-R1-Part 1.2	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use. Part 1.2: Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	<a href="#">s3-default-encryption-kms (p. 182)</a>	Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data.
CIP-011-2-R1-Part 1.2	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use. Part 1.2: Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
CIP-011-2-R1-Part 1.2	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use. Part 1.2: Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.
CIP-011-2-R1-Part 1.2	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use. Part 1.2: Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.

## Template

The template is available on GitHub: [Operational Best Practices for NERC CIP](#).

## Operational Best Practices for NCSC Cloud Security Principles

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the UK National Cyber Security Centre (NCSC) Cloud Security Principles and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more UK NCSC Cloud Security Principles controls. A UK NCSC Cloud Security Principles control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This sample conformance pack template contains mappings to controls within the UK NCSC Cloud Security Principles ([National Cyber Security Centre | Cloud security guidance](#)), with such public sector information licensed under the Open Government Licence v3.0. The Open Government Licence should can be accessed here: [Open Government Licence for public sector information](#).

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

Control ID	AWS Config Rule	Guidance
1. Data in transit protection	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.
1. Data in transit protection	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
1. Data in transit protection	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
1. Data in transit protection	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
1. Data in transit protection	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
1. Data in transit protection	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist,

Control ID	AWS Config Rule	Guidance
		enable encryption in transit to help protect that data.
1. Data in transit protection	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
1. Data in transit protection	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
2: Asset protection and resilience	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
2: Asset protection and resilience	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
2: Asset protection and resilience	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
2: Asset protection and resilience	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
2: Asset protection and resilience	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
2. Asset protection and resilience	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
2. Asset protection and resilience	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
2. Asset protection and resilience	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
2. Asset protection and resilience	<a href="#">dynamodb-table-encrypted-kms (p. 129)</a>	Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK).
2. Asset protection and resilience	<a href="#">ec2-efs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
2. Asset protection and resilience	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
2. Asset protection and resilience	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
2. Asset protection and resilience	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
2. Asset protection and resilience	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.
2. Asset protection and resilience	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.
2. Asset protection and resilience	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
2. Asset protection and resilience	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
2. Asset protection and resilience	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
2. Asset protection and resilience	<a href="#">s3-default-encryption-kms (p. 182)</a>	*DOCUMENTATION TEAM TO REVIEW*
2. Asset protection and resilience	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.
2. Asset protection and resilience	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
2. Asset protection and resilience	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.
2. Asset protection and resilience	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
5. Operational security	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
5. Operational security	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
5. Operational security	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
5. Operational security	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.

Control ID	AWS Config Rule	Guidance
5. Operational security	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
5. Operational security	<a href="#">cw-loggroup-retention-period-check (p. 125)</a>	Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events.
5. Operational security	<a href="#">ec2-imdsv2-check (p. 132)</a>	Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata.
5. Operational security	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

Control ID	AWS Config Rule	Guidance
5. Operational security	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
5. Operational security	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
5. Operational security	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
5. Operational security	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	AWS Config Rule	Guidance
5. Operational security	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.
5. Operational security	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
5. Operational security	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.

Control ID	AWS Config Rule	Guidance
5. Operational security	<a href="#">redshift-cluster-maintenancesettings-check (p. 171)</a>	<p>This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the <code>allowVersionUpgrade</code>. The default is true. It also lets you optionally set the <code>preferredMaintenanceWindow</code> (the default is <code>sat:16:00-sat:16:30</code>), and the <code>automatedSnapshotRetentionPeriod</code> (the default is 1). The actual values should reflect your organization's policies.</p>
5. Operational security	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	<p>Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.</p>
5. Operational security	<a href="#">securityhub-enabled (p. 186)</a>	<p>AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.</p>

Control ID	AWS Config Rule	Guidance
5. Operational security	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
5. Operational security	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.
5. Operational security	<a href="#">lambda-dlq-check (p. 161)</a>	Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed.
5. Operational security	<a href="#">rds-enhanced-monitoring-enabled (p. 165)</a>	Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics.

Control ID	AWS Config Rule	Guidance
7. Secure development	<a href="#">codebuild-project-envvar-awscred-check (p. 123)</a>	Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access.
7. Secure development	<a href="#">codebuild-project-source-repo-url-check (p. 123)</a>	Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, user name and password within AWS Codebuild project environments. Use OAuth instead of personal access tokens or a user name and password to grant authorization for accessing GitHub or Bitbucket repositories.
9. Secure user management	<a href="#">access-keys-rotated (p. 107)</a>	The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.
9. Secure user management	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	AWS Config Rule	Guidance
9. Secure user management	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
9. Secure user management	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
9. Secure user management	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
9. Secure user management	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	AWS Config Rule	Guidance
9. Secure user management	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.
10. Identity and authentication	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
10. Identity and authentication	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.

Control ID	AWS Config Rule	Guidance
10. Identity and authentication	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>
10. Identity and authentication	<a href="#">iam-user-mfa-enabled (p. 158)</a>	<p>Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.</p>

Control ID	AWS Config Rule	Guidance
10. Identity and authentication	<a href="#">mfa-enabled-for-iam-console-access</a> (p. 163)	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
10. Identity and authentication	<a href="#">root-account-hardware-mfa-enabled</a> (p. 175)	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
10. Identity and authentication	<a href="#">root-account-mfa-enabled</a> (p. 175)	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
10. Identity and authentication	<a href="#">secretsmanager-rotation-enabled-check</a> (p. 183)	This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised.

Control ID	AWS Config Rule	Guidance
10. Identity and authentication	<a href="#">secretsmanager-scheduled-rotation-success-check (p. 184)</a>	This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised.
11. External interface protection	<a href="#">alb-waf-enabled (p. 109)</a>	Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.
11. External interface protection	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
11. External interface protection	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
11. External interface protection	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.

Control ID	AWS Config Rule	Guidance
11. External interface protection	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
11. External interface protection	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
11. External interface protection	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
11. External interface protection	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.

Control ID	AWS Config Rule	Guidance
11. External interface protection	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
11. External interface protection	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
11. External interface protection	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
11. External interface protection	<a href="#">restricted-common-ports</a> (p. 174)	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
11. External interface protection	<a href="#">sagemaker-notebook-no-direct-internet-access</a> (p. 183)	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
11. External interface protection	<a href="#">vpc-default-security-group-closed</a> (p. 188)	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
11. External interface protection	<a href="#">vpc-sg-open-only-to-authorized-ports</a> (p. 189)	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.

Control ID	AWS Config Rule	Guidance
13. Audit information for users	<a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a>	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.
13. Audit information for users	<a href="#">cloudtrail-security-trail-enabled (p. 118)</a>	This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions.
11. External interface protection	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
11. External interface protection	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
11. External interface protection	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	AWS Config Rule	Guidance
11. External interface protection	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
13. Audit information for users	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
13. Audit information for users	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

## Template

The template is available on GitHub: [Operational Best Practices for NCSC Cloud Security Principles](#).

# Operational Best Practices for NCSC Cyber Assessment Framework

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between UK National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF) controls and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more UK NCSC CAF controls. A UK NCSC CAF control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This sample conformance pack template contains mappings to controls within the UK NCSC CAF ([National Cyber Security Centre | NCSC CAF guidance](#)), with such public sector information licensed under the Open Government Licence v3.0. The Open Government Licence should can be accessed here: [Open Government Licence for public sector information](#).

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

Control ID	AWS Config Rule	Guidance
A3.a#_Asset_Management	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
A3.a#_Asset_Management	<a href="#">ec2-stopped-instance (p. 137)</a>	Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards.
A3.a#_Asset_Management	<a href="#">ec2-volume-inuse-check (p. 137)</a>	This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality.
A3.a#_Asset_Management	<a href="#">eip-attached (p. 139)</a>	This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment.
A3.a#_Asset_Management	<a href="#">ec2-security-group-attached-to-eni (p. 137)</a>	This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the

Control ID	AWS Config Rule	Guidance
		inventory and the management of your environment.
B2.a_Identity_Verification,Authentication_and_Authorisation	check (p. 153)	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
B2.a_Identity_Verification,Authentication_and_Authorisation	check (p. 154)	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
B2.a_Identity_Verification,Authentication_and_Authorisation	with-admin-access (p. 156)	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
B2.a_Identity_Verification,Authentication_and_Authorisation	ship-check (p. 157)	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	AWS Config Rule	Guidance
B2.a_Identity_Verification,Authentication,Authorization	<a href="#">Identify Unused Credentials-check (p. 159)</a>	<p>AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies.</p>
B2.a_Identity_Verification,Authentication,Authorization	<a href="#">Require MFA for IAM Users (p. 158)</a>	<p>Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.</p>
B2.a_Identity_Verification,Authentication,Authorization	<a href="#">Require MFA for IAM Users with Console Access (p. 163)</a>	<p>Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.</p>
B2.a_Identity_Verification,Authentication,Authorization	<a href="#">Require MFA for the Root User (p. 175)</a>	<p>Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.</p>

Control ID	AWS Config Rule	Guidance
B2.a_Identity_Verification,Authentication_and_Authorisation	<a href="#">authentication and authorisation enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
B2.a_Identity_Verification,Authentication_and_Authorisation	<a href="#">check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
B2.b_Device_Management	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

Control ID	AWS Config Rule	Guidance
B2.c_Privileged_User_Management	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies.
B2.c_Privileged_User_Management	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
B2.c_Privileged_User_Management	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
B2.c_Privileged_User_Management	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	AWS Config Rule	Guidance
B2.c_Privileged_User_Management	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
B2.c_Privileged_User_Management	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
B2.c_Privileged_User_Management	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
B2.c_Privileged_User_Management	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies.

Control ID	AWS Config Rule	Guidance
B2.c_Privileged_User_Management	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
B2.c_Privileged_User_Management	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
B2.c_Privileged_User_Management	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
B2.c_Privileged_User_Management	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	AWS Config Rule	Guidance
B2.d_Identity_and_Access_Management_IAM	<a href="#">iam-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
B2.d_Identity_and_Access_Management_IAM	<a href="#">iam-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
B2.d_Identity_and_Access_Management_IAM	<a href="#">iam-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
B2.d_Identity_and_Access_Management_IAM	<a href="#">iam-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	AWS Config Rule	Guidance
B2.d_Identity_and_Access_Management_(IAM)	iam-unused-credentials-check (p. 159)	<p>AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies.</p>
B2.d_Identity_and_Access_Management_(IAM)	iam-dataevents-enabled (p. 118)	<p>The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.</p>
B2.d_Identity_and_Access_Management_(IAM)	iam-cluster-configuration-check (p. 170)	<p>To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.</p>
B2.d_Identity_and_Access_Management_(IAM)	iam-guardduty-enabled-centralized (p. 152)	<p>Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.</p>

Control ID	AWS Config Rule	Guidance
B2.d_Identity_and_Access_Management(IAM)	Non-archived-findings (p. 152)	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies.
B2.d_Identity_and_Access_Management(IAM)	Cloud-watch-logs-enabled (p. 121)	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
B2.d_Identity_and_Access_Management(IAM)	Alarm-action-check (p. 119)	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment.
B2.d_Identity_and_Access_Management(IAM)	Enabled (p. 186)	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	AWS Config Rule	Guidance
B3.a_Understanding_Data	<a href="#">ec2-volume-inuse-check (p. 137)</a>	This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality.
B3.b_Data_in_Transit	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.
B3.b_Data_in_Transit	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
B3.b_Data_in_Transit	<a href="#">alb-http-to-https-redirection-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
B3.b_Data_in_Transit	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	AWS Config Rule	Guidance
B3.b_Data_in_Transit	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
B3.b_Data_in_Transit	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
B3.b_Data_in_Transit	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
B3.b_Data_in_Transit	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
B3.b_Data_in_Transit	<a href="#">alb-waf-enabled (p. 109)</a>	Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.
B3.b_Data_in_Transit	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
B3.b_Data_in_Transit	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
B3.b_Data_in_Transit	<a href="#">ec2-security-group-attached-to-eni (p. 137)</a>	This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment.
B3.b_Data_in_Transit	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
B3.b_Data_in_Transit	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
B3.b_Data_in_Transit	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	AWS Config Rule	Guidance
B3.b_Data_in_Transit	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
B3.b_Data_in_Transit	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
B3.b_Data_in_Transit	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.

Control ID	AWS Config Rule	Guidance
B3.b_Data_in_Transit	<a href="#">rds-instance-public-access-check</a> (p. 166)	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
B3.b_Data_in_Transit	<a href="#">redshift-cluster-public-access-check</a> (p. 171)	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
B3.b_Data_in_Transit	<a href="#">restricted-common-ports</a> (p. 174)	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
B3.b_Data_in_Transit	<a href="#">sagemaker-notebook-no-direct-internet-access</a> (p. 183)	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
B3.b_Data_in_Transit	<a href="#">vpc-default-security-group-closed</a> (p. 188)	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	AWS Config Rule	Guidance
B3.b_Data_in_Transit	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
B3.b_Data_in_Transit	<a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a>	The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.
B3.b_Data_in_Transit	<a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a>	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.
B3.b_Data_in_Transit	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.

Control ID	AWS Config Rule	Guidance
B3.b_Data_in_Transit	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.
B3.c_Stored_Data	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
B3.c_Stored_Data	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
B3.c_Stored_Data	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
B3.c_Stored_Data	<a href="#">dynamodb-table-encrypted-kms (p. 129)</a>	Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK).
B3.c_Stored_Data	<a href="#">ec2-ebs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
B3.c_Stored_Data	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
B3.c_Stored_Data	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
B3.c_Stored_Data	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
B3.c_Stored_Data	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.
B3.c_Stored_Data	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.
B3.c_Stored_Data	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
B3.c_Stored_Data	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
B3.c_Stored_Data	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.
B3.c_Stored_Data	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.
B3.c_Stored_Data	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.
B3.c_Stored_Data	<a href="#">cmk-backing-key-rotation-enabled (p. 123)</a>	Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period.
B3.c_Stored_Data	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.

Control ID	AWS Config Rule	Guidance
B3.c_Stored_Data	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.
B3.c_Stored_Data	<a href="#">dynamodb-in-backup-plan (p. 128)</a>	To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
B3.c_Stored_Data	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.
B3.c_Stored_Data	<a href="#">ebs-in-backup-plan (p. 130)</a>	To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	AWS Config Rule	Guidance
B3.c_Stored_Data	<a href="#">ebs-optimized-instance (p. 131)</a>	An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance.
B3.c_Stored_Data	<a href="#">efs-in-backup-plan (p. 139)</a>	To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
B3.c_Stored_Data	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
B3.c_Stored_Data	<a href="#">rds-in-backup-plan (p. 167)</a>	To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	AWS Config Rule	Guidance
B3.c_Stored_Data	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
B3.c_Stored_Data	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.
B3.c_Stored_Data	<a href="#">rds-instance-deletion-protection-enabled (p. 166)</a>	Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
B3.c_Stored_Data	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
B3.c_Stored_Data	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
B4.a_Secure_by_Design	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.
B4.a_Secure_by_Design	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
B4.a_Secure_by_Design	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	AWS Config Rule	Guidance
B4.a_Secure_by_Design	<a href="#">alb-waf-enabled (p. 109)</a>	Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.
B4.a_Secure_by_Design	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
B4.a_Secure_by_Design	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
B4.a_Secure_by_Design	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
B4.a_Secure_by_Design	<a href="#">ec2-security-group-attached-to-eni (p. 137)</a>	This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment.

Control ID	AWS Config Rule	Guidance
B4.a_Secure_by_Design	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
B4.a_Secure_by_Design	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
B4.a_Secure_by_Design	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
B4.a_Secure_by_Design	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
B4.a_Secure_by_Design	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	AWS Config Rule	Guidance
B4.a_Secure_by_Design	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
B4.a_Secure_by_Design	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
B4.a_Secure_by_Design	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
B4.a_Secure_by_Design	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	AWS Config Rule	Guidance
B4.a_Secure_by_Design	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
B4.a_Secure_by_Design	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
B4.a_Secure_by_Design	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
B4.a_Secure_by_Design	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
B4.a_Secure_by_Design	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
B4.a_Secure_by_Design	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
B4.a_Secure_by_Design	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
B4.a_Secure_by_Design	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	AWS Config Rule	Guidance
B4.a_Secure_by_Design	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
B4.a_Secure_by_Design	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
B4.a_Secure_by_Design	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
B4.a_Secure_by_Design	<a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a>	The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.

Control ID	AWS Config Rule	Guidance
B4.a_Secure_by_Design	<a href="#">dynamodb-autoscaling-enabled (p. 128)</a>	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.
B4.a_Secure_by_Design	<a href="#">dynamodb-throughput-limit-check (p. 130)</a>	Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set <code>accountRCUThresholdPercentage</code> (Config Default: 80) and <code>accountWCUThresholdPercentage</code> (Config Default: 80) parameters. The actual values should reflect your organization's policies.
B4.a_Secure_by_Design	<a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a>	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.
B4.a_Secure_by_Design	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.

Control ID	AWS Config Rule	Guidance
B4.a_Secure_by_Design	<a href="#">lambda-concurrency-check (p. 161)</a>	This rule ensures that a Lambda function's concurrency high and low limits are established. This can assist in baselining the number of requests that your function is serving at any given time.
B4.a_Secure_by_Design	<a href="#">rds-instance-deletion-protection-enabled (p. 166)</a>	Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
B4.a_Secure_by_Design	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
B4.a_Secure_by_Design	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.

Control ID	AWS Config Rule	Guidance
B4.a_Secure_by_Design	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.
B4.b_Secure_Configuration	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
B4.b_Secure_Configuration	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.

Control ID	AWS Config Rule	Guidance
B4.b_Secure_Configuration	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
B4.b_Secure_Configuration	<a href="#">ec2-imdsv2-check (p. 132)</a>	Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata.
B4.b_Secure_Configuration	<a href="#">redshift-cluster-maintenancesettings-check (p. 171)</a>	This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferredMaintenanceWindow (the default is sat:16:00-sat:16:30), and the automatedSnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
B4.c#_Secure_Management	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
B4.c#_Secure_Management	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
B4.c#_Secure_Management	<a href="#">ec2-imdsv2-check (p. 132)</a>	Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata.
B4.d._Vulnerability_Management	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

Control ID	AWS Config Rule	Guidance
B4.d._Vulnerability_Management	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
B4.d._Vulnerability_Management	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
B4.d._Vulnerability_Management	<a href="#">ec2-imdsv2-check (p. 132)</a>	Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata.

Control ID	AWS Config Rule	Guidance
B4.d._Vulnerability_Management	<a href="#">redshift-cluster-maintenancesettings-check (p. 171)</a>	<p>This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the <code>allowVersionUpgrade</code>. The default is <code>true</code>. It also lets you optionally set the <code>preferredMaintenanceWindow</code> (the default is <code>sat:16:00-sat:16:30</code>), and the <code>automatedSnapshotRetentionPeriod</code> (the default is <code>1</code>). The actual values should reflect your organization's policies.</p>
B4.d._Vulnerability_Management	<a href="#">securityhub-enabled (p. 186)</a>	<p>AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.</p>
B5.b_Design_for_Resilience	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	<p>Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.</p>

Control ID	AWS Config Rule	Guidance
B5.b_Design_for_Resilience	<a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a>	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.
B5.b_Design_for_Resilience	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
B5.c_Backups	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.

Control ID	AWS Config Rule	Guidance
B5.c_Backups	<a href="#">dynamodb-in-backup-plan (p. 128)</a>	To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
B5.c_Backups	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.
B5.c_Backups	<a href="#">ebs-in-backup-plan (p. 130)</a>	To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
B5.c_Backups	<a href="#">ebs-optimized-instance (p. 131)</a>	An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance.

Control ID	AWS Config Rule	Guidance
B5.c_Backups	<a href="#">efs-in-backup-plan (p. 139)</a>	To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
B5.c_Backups	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
B5.c_Backups	<a href="#">rds-in-backup-plan (p. 167)</a>	To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
B5.c_Backups	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.

Control ID	AWS Config Rule	Guidance
B5.c_Backups	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.
C1.a_Monitoring_Coverage	<a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a>	The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.
C1.a_Monitoring_Coverage	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
C1.a_Monitoring_Coverage	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.

Control ID	AWS Config Rule	Guidance
C1.a_Monitoring_Coverage	<a href="#">dynamodb-throughput-limit-check (p. 130)</a>	Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set <code>accountRCUThresholdPercentage</code> (Config Default: 80) and <code>accountWCUThresholdPercentage</code> (Config Default: 80) parameters. The actual values should reflect your organization's policies.
C1.a_Monitoring_Coverage	<a href="#">ec2-instance-detailed-monitoring-enabled (p. 132)</a>	Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance.
C1.a_Monitoring_Coverage	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
C1.a_Monitoring_Coverage	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.

Control ID	AWS Config Rule	Guidance
C1.a_Monitoring_Coverage	<a href="#">lambda-concurrency-check (p. 161)</a>	This rule ensures that a Lambda function's concurrency high and low limits are established. This can assist in baselining the number of requests that your function is serving at any given time.
C1.a_Monitoring_Coverage	<a href="#">lambda-dlq-check (p. 161)</a>	Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed.
C1.a_Monitoring_Coverage	<a href="#">rds-enhanced-monitoring-enabled (p. 165)</a>	Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics.
C1.a_Monitoring_Coverage	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	AWS Config Rule	Guidance
C1.b_Securing_Logs	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.
C1.b_Securing_Logs	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
C1.b_Securing_Logs	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
C1.b_Securing_Logs	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
C1.b_Securing_Logs	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	AWS Config Rule	Guidance
C1.b_Securing_Logs	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
C1.b_Securing_Logs	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
C1.b_Securing_Logs	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
C1.b_Securing_Logs	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	AWS Config Rule	Guidance
C1.b_Securing_Logs	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
C1.b_Securing_Logs	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.
C1.c_Generating_Alerts	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
C1.c_Generating_Alerts	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.

Control ID	AWS Config Rule	Guidance
C1.c_Generating_Alerts	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
C1.c_Generating_Alerts	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
C1.c_Generating_Alerts	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
C1.c_Generating_Alerts	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
C1.c_Generating_Alerts	<a href="#">cloudtrail-security-trail-enabled (p. 118)</a>	This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions.
C1.c_Generating_Alerts	<a href="#">cw-loggroup-retention-period-check (p. 125)</a>	Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events.

Control ID	AWS Config Rule	Guidance
C1.c_Generating_Alerts	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
C1.c_Generating_Alerts	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
C1.c_Generating_Alerts	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
C1.c_Generating_Alerts	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
C1.c_Generating_Alerts	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
C1.c_Generating_Alerts	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.
C1.d_Identifying_Security_Incidents	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	AWS Config Rule	Guidance
C1.d_Identifying_Security_Incident	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
C1.e _Monitoring_Tools_and_Skills	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
C1.e _Monitoring_Tools_and_Skills	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.
C1.e _Monitoring_Tools_and_Skills	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	AWS Config Rule	Guidance
C2.a_System_Abnormalities_for_Attack_Detection-enabled-centralized (p. 152)		Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
C2.a_System_Abnormalities_for_Attack_Detection-enabled (p. 186)		AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

## Template

The template is available on GitHub: [Operational Best Practices for NCSC Cyber Assessment Framework](#).

## Operational Best Practices for Networking and Content Delivery Services

This pack contains AWS Config rules based on Networking and Content Delivery Services. For more information, see [Networking and Content Delivery on AWS](#). This Conformance Pack has been designed for compatibility with the majority of AWS regions and to not require setting of any Parameters. Additional managed rules that require parameters to be set for your environment and/or for your specific region can be found at: [List of AWS Config Managed Rules](#).

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

See Parameters section for names and descriptions of required parameters.

The template is available on GitHub: [Operational Best Practices for Networking and Content Delivery Services](#).

## Operational Best Practices for NIST 800-53 rev 4

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the NIST 800-53 and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more NIST 800-53 controls. A NIST 800-53 control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This Conformance Pack was validated by AWS Security Assurance Services LLC (AWS SAS), which is a team of Payment Card Industry Qualified Security Assessors (QSAs), HITRUST Certified Common Security Framework Practitioners (CCSFPs), and compliance professionals certified to provide guidance and assessments for various industry frameworks. AWS SAS professionals designed this Conformance Pack to enable a customer to align to a subset of the NIST 800-53.

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

Control ID	Control Description	AWS Config Rule	Guidance
AC-2(1)	The organization employs automated mechanisms to support the management of information system accounts.	<a href="#">secretsmanager-scheduled-rotation-success-check (p. 184)</a>	This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised.
AC-2(1)	The organization employs automated mechanisms to support the management of information system accounts.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC-2(1)	The organization employs automated mechanisms to support the management of information system accounts.	<a href="#">iam-password-policy (p. 154)</a>	The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength.

Control ID	Control Description	AWS Config Rule	Guidance
			<p>This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AC-2(1)	The organization employs automated mechanisms to support the management of information system accounts.	<a href="#">access-keys-rotated (p. 107)</a>	The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.
AC-2(1)	The organization employs automated mechanisms to support the management of information system accounts.	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AC-2(1)	The organization employs automated mechanisms to support the management of information system accounts.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
AC-2(1)	The organization employs automated mechanisms to support the management of information system accounts.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
AC-2(3)	The information system automatically disables inactive accounts after [Assignment: organization-defined time period].	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.
AC-2(4)	The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles].	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
AC-2(4)	The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles].	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
AC-2(4)	The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles].	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
AC-2(4)	The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles].	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	Control Description	AWS Config Rule	Guidance
AC-2(4)	The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles].	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
AC-2(4)	The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles].	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.

Control ID	Control Description	AWS Config Rule	Guidance
AC-2(4)	The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles].	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
AC-2(4)	The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles].	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AC-2(12)(a)	The organization: a. Monitors information system accounts for [Assignment: organization-defined atypical use].	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
AC-2(12)(a)	The organization: a. Monitors information system accounts for [Assignment: organization-defined atypical use].	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
AC-2(f)	The organization: f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions].	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AC-2(f)	<p>The organization: f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions].</p>	<p><a href="#">iam-password-policy (p. 154)</a></p>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AC-2(f)	The organization: f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions].	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
AC-2(g)	The organization: g. Monitors the use of information system accounts.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AC-2(g)	The organization: g. Monitors the use of information system accounts.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
AC-2(g)	The organization: g. Monitors the use of information system accounts.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
AC-2(g)	The organization: g. Monitors the use of information system accounts.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.

Control ID	Control Description	AWS Config Rule	Guidance
AC-2(g)	The organization: g. Monitors the use of information system accounts.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
AC-2(g)	The organization: g. Monitors the use of information system accounts.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
AC-2(g)	The organization: g. Monitors the use of information system accounts.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.

Control ID	Control Description	AWS Config Rule	Guidance
AC-2(g)	The organization: g. Monitors the use of information system accounts.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
AC-2(j)	The organization: j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency].	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
AC-2(j)	The organization: j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency].	<a href="#">secretsmanager-scheduled-rotation-success-check (p. 184)</a>	This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised.
AC-2(j)	The organization: j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency].	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
AC-2(j)	<p>The organization: j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency].</p>	<p><a href="#">iam-password-policy (p. 154)</a></p>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AC-2(j)	The organization: j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency].	<a href="#">access-keys-rotated (p. 107)</a>	The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.
AC-2(j)	The organization: j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency].	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.

Control ID	Control Description	AWS Config Rule	Guidance
AC-2(j)	<p>The organization: j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency].</p>	<p><a href="#">emr-kerberos-enabled (p. 145)</a></p>	<p>The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.</p>
AC-2(j)	<p>The organization: j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency].</p>	<p><a href="#">iam-group-has-users-check (p. 153)</a></p>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AC-2(j)	The organization: j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency].	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC-2(j)	The organization: j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency].	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.
AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.

Control ID	Control Description	AWS Config Rule	Guidance
AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	Control Description	AWS Config Rule	Guidance
AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC-3	The information system enforces approved authorizations for information and system resources in accordance with applicable access control policies.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.

Control ID	Control Description	AWS Config Rule	Guidance
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.

Control ID	Control Description	AWS Config Rule	Guidance
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
AC-5c	The organization: c. Defines information system access authorizations to support separation of duties.	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.

Control ID	Control Description	AWS Config Rule	Guidance
AC-5c	The organization: c. Defines information system access authorizations to support separation of duties.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
AC-5c	The organization: c. Defines information system access authorizations to support separation of duties.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC-5c	The organization: c. Defines information system access authorizations to support separation of duties.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	Control Description	AWS Config Rule	Guidance
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling s3_bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">codebuild-project-envvar-awscred-check (p. 123)</a>	Ensure authentication credentials <code>AWS_ACCESS_KEY_ID</code> and <code>AWS_SECRET_ACCESS_KEY</code> do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access.

Control ID	Control Description	AWS Config Rule	Guidance
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	Control Description	AWS Config Rule	Guidance
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">ec2-imdsv2-check (p. 132)</a>	Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata.
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
AC-6(10)	The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.

Control ID	Control Description	AWS Config Rule	Guidance
AC-17(1)	The information system monitors and controls remote access methods.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
AC-17(1)	The information system monitors and controls remote access methods.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
AC-17(2)	The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
AC-17(2)	The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
AC-17(2)	The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.
AC-17(2)	The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
AC-17(2)	The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.

Control ID	Control Description	AWS Config Rule	Guidance
AC-17(2)	The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
AC-17(2)	The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
AC-17(3)	The information system routes all remote accesses through [Assignment: organization-defined number] managed network access control points.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
AC-21(b)	The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/ collaboration decisions.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
AC-21(b)	The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/ collaboration decisions.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC-21(b)	The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/ collaboration decisions.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
AC-21(b)	The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/ collaboration decisions.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
AC-21(b)	The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/ collaboration decisions.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
AC-21(b)	The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/ collaboration decisions.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
AC-21(b)	The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/ collaboration decisions.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
AC-21(b)	The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/ collaboration decisions.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
AC-21(b)	The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/ collaboration decisions.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
AC-21(b)	The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/ collaboration decisions.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC-21(b)	The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/ collaboration decisions.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
AC-21(b)	The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/ collaboration decisions.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
AU-2(a)(d)	The organization: a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events]; d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event].	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
AU-2(a)(d)	The organization: a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events]; d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event].	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
AU-2(a)(d)	<p>The organization:</p> <p>a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events];</p> <p>d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event].</p>	<p><a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a></p>	<p>The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.</p>
AU-2(a)(d)	<p>The organization:</p> <p>a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events];</p> <p>d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event].</p>	<p><a href="#">cloudtrail-enabled (p. 121)</a></p>	<p>AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AU-2(a)(d)	<p>The organization:</p> <p>a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events];</p> <p>d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event].</p>	<p><a href="#">elb-logging-enabled (p. 144)</a></p>	<p>Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.</p>
AU-2(a)(d)	<p>The organization:</p> <p>a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events];</p> <p>d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event].</p>	<p><a href="#">multi-region-cloudtrail-enabled (p. 163)</a></p>	<p>AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AU-2(a)(d)	<p>The organization:</p> <p>a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events];</p> <p>d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event].</p>	<p><a href="#">s3-bucket-logging-enabled (p. 177)</a></p>	<p>Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.</p>
AU-2(a)(d)	<p>The organization:</p> <p>a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events];</p> <p>d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event].</p>	<p><a href="#">vpc-flow-logs-enabled (p. 188)</a></p>	<p>The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AU-2(a)(d)	<p>The organization:</p> <p>a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events];</p> <p>d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event].</p>	<p><a href="#">rds-logging-enabled (p. 167)</a></p>	<p>To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.</p>
AU-2(a)(d)	<p>The organization:</p> <p>a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events];</p> <p>d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event].</p>	<p><a href="#">wafv2-logging-enabled (p. 190)</a></p>	<p>To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AU-2(a)(d)	The organization: a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events]; d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event].	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
AU-3	The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
AU-3	The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
AU-3	The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
AU-3	The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
AU-3	The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	Control Description	AWS Config Rule	Guidance
AU-3	The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
AU-3	The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.

Control ID	Control Description	AWS Config Rule	Guidance
AU-3	The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
AU-3	The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.

Control ID	Control Description	AWS Config Rule	Guidance
AU-3	The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
AU-3	The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.

Control ID	Control Description	AWS Config Rule	Guidance
AU-6(1)(3)	(1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
AU-6(1)(3)	(1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
AU-6(1)(3)	(1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), and <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
AU-6(1)(3)	(1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
AU-7(1)	The information system provides the capability to process audit records for events of interest based on [Assignment: organization-defined audit fields within audit records].	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
AU-7(1)	The information system provides the capability to process audit records for events of interest based on [Assignment: organization-defined audit fields within audit records].	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
AU-9	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
AU-9	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.

Control ID	Control Description	AWS Config Rule	Guidance
AU-9(2)	The information system backs up audit records [Assignment: organization-defined frequency] onto a physically different system or system component than the system or component being audited.	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
AU-11	The organization retains audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	<a href="#">cw-loggroup-retention-period-check (p. 125)</a>	Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events.
AU-12(a)(c)	The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at [Assignment: organization-defined information system components]; c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.

Control ID	Control Description	AWS Config Rule	Guidance
AU-12(a)(c)	The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at [Assignment: organization-defined information system components]; c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
AU-12(a)(c)	The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at [Assignment: organization-defined information system components]; c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
AU-12(a)(c)	The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at [Assignment: organization-defined information system components]; c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.

Control ID	Control Description	AWS Config Rule	Guidance
AU-12(a)(c)	The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at [Assignment: organization-defined information system components]; c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
AU-12(a)(c)	The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at [Assignment: organization-defined information system components]; c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
AU-12(a)(c)	<p>The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at [Assignment: organization-defined information system components]; c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.</p>	<p><a href="#">multi-region-cloudtrail-enabled (p. 163)</a></p>	<p>AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.</p>
AU-12(a)(c)	<p>The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at [Assignment: organization-defined information system components]; c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.</p>	<p><a href="#">s3-bucket-logging-enabled (p. 177)</a></p>	<p>Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.</p>

Control ID	Control Description	AWS Config Rule	Guidance
AU-12(a)(c)	The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at [Assignment: organization-defined information system components]; c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
AU-12(a)(c)	The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at [Assignment: organization-defined information system components]; c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.

Control ID	Control Description	AWS Config Rule	Guidance
AU-12(a)(c)	<p>The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at [Assignment: organization-defined information system components]; c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.</p>	<p><a href="#">redshift-cluster-configuration-check (p. 170)</a></p>	<p>To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.</p>
CA-7(a)(b)	<p>The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:</p> <ul style="list-style-type: none"> <li>a. Establishment of [Assignment: organization-defined metrics] to be monitored;</li> <li>b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring</li> </ul>	<p><a href="#">guardduty-enabled-centralized (p. 152)</a></p>	<p>Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.</p>

Control ID	Control Description	AWS Config Rule	Guidance
CA-7(a)(b)	<p>The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:</p> <ul style="list-style-type: none"> <li>a. Establishment of [Assignment: organization-defined metrics] to be monitored;</li> <li>b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring.</li> </ul>	<a href="#">securityhub-enabled (p. 186)</a>	<p>AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.</p>
CA-7(a)(b)	<p>The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:</p> <ul style="list-style-type: none"> <li>a. Establishment of [Assignment: organization-defined metrics] to be monitored;</li> <li>b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring.</li> </ul>	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	<p>Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.</p>

Control ID	Control Description	AWS Config Rule	Guidance
CA-7(a)(b)	<p>The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:</p> <ul style="list-style-type: none"> <li>a. Establishment of [Assignment: organization-defined metrics] to be monitored;</li> <li>b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring.</li> </ul>	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	<p>Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), and <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.</p>
CA-7(a)(b)	<p>The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:</p> <ul style="list-style-type: none"> <li>a. Establishment of [Assignment: organization-defined metrics] to be monitored;</li> <li>b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring.</li> </ul>	<a href="#">ec2-instance-detailed-monitoring-enabled (p. 132)</a>	<p>Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance.</p>

Control ID	Control Description	AWS Config Rule	Guidance
CA-7(a)(b)	The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring.	<a href="#">rds-enhanced-monitoring-enabled (p. 165)</a>	Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics.
CM-2	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
CM-2	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
CM-2	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	<a href="#">ec2-stopped-instance (p. 137)</a>	Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards.
CM-2	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	<a href="#">ec2-volume-inuse-check (p. 137)</a>	This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality.

Control ID	Control Description	AWS Config Rule	Guidance
CM-2	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
CM-2	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
CM-2	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	<a href="#">cloudtrail-security-trail-enabled (p. 118)</a>	This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions.

Control ID	Control Description	AWS Config Rule	Guidance
CM-7(a)	The organization: a. Configures the information system to provide only essential capabilities.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
CM-7(a)	The organization: a. Configures the information system to provide only essential capabilities.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
CM-8(1)	The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
CM-8(3)(a)	The organization: a. Employs automated mechanisms [Assignment: organization-defined frequency] to detect the presence of unauthorized hardware, software, and firmware components within the information system	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
CM-8(3)(a)	The organization: a. Employs automated mechanisms [Assignment: organization-defined frequency] to detect the presence of unauthorized hardware, software, and firmware components within the information system	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
CM-8(3)(a)	The organization: a. Employs automated mechanisms [Assignment: organization-defined frequency] to detect the presence of unauthorized hardware, software, and firmware components within the information system	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
CP-9(b)	The organization: b. Conducts backups of system-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives].	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.

Control ID	Control Description	AWS Config Rule	Guidance
CP-9(b)	The organization: b. Conducts backups of system-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives].	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.
CP-9(b)	The organization: b. Conducts backups of system-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives].	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
CP-9(b)	The organization: b. Conducts backups of system-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives].	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.

Control ID	Control Description	AWS Config Rule	Guidance
CP-9(b)	The organization: b. Conducts backups of system-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives].	<a href="#">dynamodb-in-backup-plan (p. 128)</a>	To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
CP-9(b)	The organization: b. Conducts backups of system-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives].	<a href="#">ebs-in-backup-plan (p. 130)</a>	To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
CP-9(b)	The organization: b. Conducts backups of system-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives].	<a href="#">efs-in-backup-plan (p. 139)</a>	To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	Control Description	AWS Config Rule	Guidance
CP-9(b)	The organization: b. Conducts backups of system-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives].	<a href="#">rds-in-backup-plan (p. 167)</a>	To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	<a href="#">dynamodb-autoscaling-enabled (p. 128)</a>	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.
CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.

Control ID	Control Description	AWS Config Rule	Guidance
CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.

Control ID	Control Description	AWS Config Rule	Guidance
CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.
CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.
CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.

Control ID	Control Description	AWS Config Rule	Guidance
CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	<a href="#">dynamodb-in-backup-plan (p. 128)</a>	To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	Control Description	AWS Config Rule	Guidance
CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	<a href="#">ebs-in-backup-plan (p. 130)</a>	To help with data backup processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	<a href="#">efs-in-backup-plan (p. 139)</a>	To help with data backup processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	<a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a>	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.

Control ID	Control Description	AWS Config Rule	Guidance
CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	<a href="#">rds-in-backup-plan (p. 167)</a>	To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	Control Description	AWS Config Rule	Guidance
IA-2	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
IA-2(1)(11)	(1) The information system implements multifactor authentication for network access to privileged accounts. (11) The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [Assignment: organization-defined strength of mechanism requirements].	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
IA-2(1)(11)	(1) The information system implements multifactor authentication for network access to privileged accounts. (11) The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [Assignment: organization-defined strength of mechanism requirements].	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	Control Description	AWS Config Rule	Guidance
IA-2(1)(2)(11)	<p>(1) The information system implements multifactor authentication for network access to privileged accounts. (2) The information system implements multifactor authentication for network access to non- privileged accounts. (11) The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [Assignment: organization-defined strength of mechanism requirements].</p>	<p><a href="#">mfa-enabled-for-iam-console-access (p. 163)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.</p>
IA-2(1)(2)(11)	<p>(1) The information system implements multifactor authentication for network access to privileged accounts. (2) The information system implements multifactor authentication for network access to non- privileged accounts. (11) The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [Assignment: organization-defined strength of mechanism requirements].</p>	<p><a href="#">iam-user-mfa-enabled (p. 158)</a></p>	<p>Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.</p>

Control ID	Control Description	AWS Config Rule	Guidance
IA-5(1)(a)(d)(e)	<p>The information system, for password-based authentication:</p> <p>a. Enforces minimum password complexity of [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type]; d. Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum]; e. Prohibits password reuse for [Assignment: organization-defined number] generations.</p>	<p><a href="#">iam-password-policy (p. 154)</a></p>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
IA-5(4)	The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy [Assignment: organization-defined requirements].	<a href="#">iam-password-policy (p. 154)</a>	The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
IA-5(7)	The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.	<a href="#">codebuild-project-envvar-awscred-check (p. 123)</a>	Ensure authentication credentials <code>AWS_ACCESS_KEY_ID</code> and <code>AWS_SECRET_ACCESS_KEY</code> do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access.
IR-4(1)	The organization employs automated mechanisms to support the incident handling process.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.

Control ID	Control Description	AWS Config Rule	Guidance
IR-4(1)	The organization employs automated mechanisms to support the incident handling process.	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.
IR-6(1)	The organization employs automated mechanisms to assist in the reporting of security incidents.	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
IR-7(1)	The organization employs automated mechanisms to increase the availability of incident response-related information and support.	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
RA-5	<p>The organization: a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities [Assignment: organization-defined response times], in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate</p>	<p><a href="#">guardduty-enabled-centralized (p. 152)</a></p>	<p>Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).		

Control ID	Control Description	AWS Config Rule	Guidance
RA-5	<p>The organization: a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities [Assignment: organization-defined response times], in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate</p>	<p><a href="#">guardduty-non-archived-findings (p. 152)</a></p>	<p>Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
	similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).		
SA-3(a)	The organization: a. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations.	<a href="#">codebuild-project-envvar-awscred-check (p. 123)</a>	Ensure authentication credentials <code>AWS_ACCESS_KEY_ID</code> and <code>AWS_SECRET_ACCESS_KEY</code> do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access.
SA-3(a)	The organization: a. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
SA-3(a)	The organization: a. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations.	<a href="#">codebuild-project-source-repo-url-check (p. 123)</a>	Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, user name and password within AWS Codebuild project environments. Use OAuth instead of personal access tokens or a user name and password to grant authorization for accessing GitHub or Bitbucket repositories.

Control ID	Control Description	AWS Config Rule	Guidance
SA-10	<p>The organization requires the developer of the information system, system component, or information system service to:</p> <ul style="list-style-type: none"><li>a. Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation];</li><li>b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management];</li><li>c. Implement only organization-approved changes to the system, component, or service;</li><li>d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and</li><li>e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].</li></ul>	<a href="#">guardduty-enabled-centralized (p. 152)</a>	<p>Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SA-10	<p>The organization requires the developer of the information system, system component, or information system service to: a. Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation]; b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management]; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].</p>	<p><a href="#">guardduty-non-archived-findings (p. 152)</a></p>	<p>Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SA-10	<p>The organization requires the developer of the information system, system component, or information system service to:</p> <ul style="list-style-type: none"><li>a. Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation];</li><li>b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management];</li><li>c. Implement only organization-approved changes to the system, component, or service;</li><li>d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and</li><li>e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].</li></ul>	<p><a href="#">securityhub-enabled (p. 186)</a></p>	<p>AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SA-10	<p>The organization requires the developer of the information system, system component, or information system service to:</p> <ul style="list-style-type: none"><li>a. Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation];</li><li>b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management];</li><li>c. Implement only organization-approved changes to the system, component, or service;</li><li>d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and</li><li>e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].</li></ul>	<p><a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a></p>	<p>An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SC-2	The information system separates user functionality (including user interface services) from information system management functionality.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
SC-2	The information system separates user functionality (including user interface services) from information system management functionality.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
SC-4	The information system prevents unauthorized and unintended information transfer via shared system resources.	<a href="#">ec2-volume-inuse-check (p. 137)</a>	This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality.
SC-5	The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards].	<a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a>	The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.
SC-5	The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards].	<a href="#">dynamodb-autoscaling-enabled (p. 128)</a>	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.

Control ID	Control Description	AWS Config Rule	Guidance
SC-5	The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards].	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
SC-5	The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards].	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.

Control ID	Control Description	AWS Config Rule	Guidance
SC-5	The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards].	<a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a>	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.
SC-5	The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards].	<a href="#">rds-instance-deletion-protection-enabled (p. 166)</a>	Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.

Control ID	Control Description	AWS Config Rule	Guidance
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">ec2-instance-no-public-ip (p. 133)</a></p>	<p>Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.</p>
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">s3-bucket-ssl-requests-only (p. 181)</a></p>	<p>To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">redshift-require-tls-ssl (p. 172)</a></p>	<p>Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.</p>
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">elb-acm-certificate-required (p. 143)</a></p>	<p>Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">alb-http-to-https-redirect-check (p. 109)</a></p>	<p>To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.</p>
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">elb-tls-https-listeners-only (p. 145)</a></p>	<p>Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SC-7	The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.

Control ID	Control Description	AWS Config Rule	Guidance
SC-7	The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.

Control ID	Control Description	AWS Config Rule	Guidance
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">internet-gateway-authorized-vpc-only (p. 160)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.</p>
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">dms-replication-not-public (p. 127)</a></p>	<p>Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">ebs-snapshot-public-restorable-check (p. 131)</a></p>	<p>Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.</p>
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">elasticsearch-in-vpc-only (p. 141)</a></p>	<p>Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">emr-master-no-public-ip (p. 146)</a></p>	<p>Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.</p>
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">restricted-ssh (p. 159)</a></p>	<p>Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">lambda-function-public-access-prohibited (p. 161)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.</p>
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">lambda-inside-vpc (p. 162)</a></p>	<p>Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">rds-instance-public-access-check (p. 166)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.</p>
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">rds-snapshots-public-prohibited (p. 168)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">redshift-cluster-public-access-check (p. 171)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.</p>
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">restricted-common-ports (p. 174)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">s3-bucket-public-read-prohibited (p. 179)</a></p>	<p>Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.</p>
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">s3-bucket-public-write-prohibited (p. 180)</a></p>	<p>Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.</p>
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">vpc-default-security-group-closed (p. 188)</a></p>	<p>Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">alb-waf-enabled (p. 109)</a></p>	<p>Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.</p>
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">s3-bucket-policy-grantee-check (p. 178)</a></p>	<p>Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code>. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">s3-account-level-public-access-blocks (p. 175)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.</p>
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a></p>	<p>Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a></p>	<p>Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.</p>
SC-7	<p>The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.</p>	<p><a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a></p>	<p>Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.

Control ID	Control Description	AWS Config Rule	Guidance
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.

Control ID	Control Description	AWS Config Rule	Guidance
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling s3_bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	Control Description	AWS Config Rule	Guidance
SC-7(3)	The organization limits the number of external network connections to the information system.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
SC-8	The information system protects the [Selection (one or more): confidentiality; integrity] of transmitted information.	<a href="#">alb-http-to-https-redirection-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC-8	The information system protects the [Selection (one or more): confidentiality; integrity] of transmitted information.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC-8	The information system protects the [Selection (one or more): confidentiality; integrity] of transmitted information.	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SC-8	The information system protects the [Selection (one or more): confidentiality; integrity] of transmitted information.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC-8	The information system protects the [Selection (one or more): confidentiality; integrity] of transmitted information.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC-8	The information system protects the [Selection (one or more): confidentiality; integrity] of transmitted information.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
SC-8	The information system protects the [Selection (one or more): confidentiality; integrity] of transmitted information.	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.

Control ID	Control Description	AWS Config Rule	Guidance
SC-8(1)	The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards].	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC-8(1)	The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards].	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC-8(1)	The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards].	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SC-8(1)	The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards].	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC-8(1)	The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards].	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC-8(1)	The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards].	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SC-8(1)	The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards].	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
SC-12	The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].	<a href="#">cmk-backing-key-rotation-enabled (p. 123)</a>	Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period.
SC-12	The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
SC-12	The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.
SC-13	The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
SC-13	The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	<a href="#">alb-http-to-https-redirection-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SC-13	The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
SC-13	The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
SC-13	The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
SC-13	The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).

Control ID	Control Description	AWS Config Rule	Guidance
SC-13	The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
SC-13	The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
SC-13	The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SC-13	The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
SC-13	The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC-13	The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SC-13	The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
SC-13	The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.
SC-13	The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SC-13	The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.
SC-13	The information system implements FIPS-validated or NSA-approved cryptography in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	<a href="#">dynamodb-table-encrypted-kms (p. 129)</a>	Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK).
SC-23	The information system protects the authenticity of communications sessions.	<a href="#">alb-http-to-https-redirection-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC-23	The information system protects the authenticity of communications sessions.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SC-23	The information system protects the authenticity of communications sessions.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
SC-28	The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest].	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
SC-28	The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest].	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
SC-28	The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest].	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
SC-28	The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest].	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
SC-28	The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest].	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.

Control ID	Control Description	AWS Config Rule	Guidance
SC-28	The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest].	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
SC-28	The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest].	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.
SC-28	The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest].	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
SC-28	The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest].	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.
SC-28	The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest].	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
SC-28	The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest].	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.
SC-28	The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest].	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SC-28	The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest].	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.
SC-28	The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest].	<a href="#">ec2-ebs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
SC-28	The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest].	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.
SC-28	The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest].	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
SC-36	The organization distributes [Assignment: organization-defined processing and storage] across multiple physical locations.	<a href="#">rds-multi-az- support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
SC-36	The organization distributes [Assignment: organization-defined processing and storage] across multiple physical locations.	<a href="#">s3-bucket-replication- enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.

Control ID	Control Description	AWS Config Rule	Guidance
SI-2(2)	The organization employs automated mechanisms [Assignment: organization-defined frequency] to determine the state of information system components with regard to flaw remediation.	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
SI-2(2)	The organization employs automated mechanisms [Assignment: organization-defined frequency] to determine the state of information system components with regard to flaw remediation.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
SI-2(2)	The organization employs automated mechanisms [Assignment: organization-defined frequency] to determine the state of information system components with regard to flaw remediation.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
SI-4(1)	The organization connects and configures individual intrusion detection tools into an information system-wide intrusion detection system.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
SI-4(2)	The organization employs automated tools to support near real-time analysis of events.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
SI-4(2)	The organization employs automated tools to support near real-time analysis of events.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
SI-4(2)	The organization employs automated tools to support near real-time analysis of events.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
SI-4(2)	The organization employs automated tools to support near real-time analysis of events.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
SI-4(2)	The organization employs automated tools to support near real-time analysis of events.	<a href="#">ec2-instance-detailed-monitoring-enabled (p. 132)</a>	Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance.

Control ID	Control Description	AWS Config Rule	Guidance
SI-4(4)	The information system monitors inbound and outbound communications traffic [Assignment: organization-defined frequency] for unusual or unauthorized activities or conditions.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
SI-4(4)	The information system monitors inbound and outbound communications traffic [Assignment: organization-defined frequency] for unusual or unauthorized activities or conditions.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
SI-4(4)	The information system monitors inbound and outbound communications traffic [Assignment: organization-defined frequency] for unusual or unauthorized activities or conditions.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
SI-4(4)	The information system monitors inbound and outbound communications traffic [Assignment: organization-defined frequency] for unusual or unauthorized activities or conditions.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
SI-4(5)	The information system alerts [Assignment: organization-defined personnel or roles] when the following indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators].	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
SI-4(5)	The information system alerts [Assignment: organization-defined personnel or roles] when the following indications of compromise or potential compromise occur: [Assignment: organization- defined compromise indicators].	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
SI-4(5)	The information system alerts [Assignment: organization-defined personnel or roles] when the following indications of compromise or potential compromise occur: [Assignment: organization- defined compromise indicators].	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.

Control ID	Control Description	AWS Config Rule	Guidance
SI-4(5)	The information system alerts [Assignment: organization-defined personnel or roles] when the following indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators].	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
SI-4(16)	The organization correlates information from monitoring tools employed throughout the information system.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
SI-4(16)	The organization correlates information from monitoring tools employed throughout the information system.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
SI-4(a)(b)(c)	The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization- defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization- determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
SI-4(a)(b)(c)	<p>The organization:</p> <p>a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization- defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization- determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization.</p>	<p><a href="#">guardduty-non-archived-findings (p. 152)</a></p>	<p>Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SI-4(a)(b)(c)	The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization- defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization- determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization.	<a href="#">alb-waf-enabled (p. 109)</a>	Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.

Control ID	Control Description	AWS Config Rule	Guidance
SI-4(a)(b)(c)	<p>The organization:</p> <p>a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization- defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization- determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization.</p>	<p><a href="#">wafv2-logging-enabled (p. 190)</a></p>	<p>To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SI-4(a)(b)(c)	<p>The organization:</p> <p>a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization- defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization- determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization.</p>	<p><a href="#">securityhub-enabled (p. 186)</a></p>	<p>AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SI-4(a)(b)(c)	<p>The organization:</p> <p>a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization- defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization- determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization.</p>	<p><a href="#">cloudwatch-alarm-action-check (p. 119)</a></p>	<p>Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), and <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SI-4(a)(b)(c)	The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization- defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization- determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
SI-4(a)(b)(c)	<p>The organization:</p> <p>a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization- defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization- determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization.</p>	<p><a href="#">ec2-instance-detailed-monitoring-enabled (p. 132)</a></p>	<p>Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance.</p>
SI-7	<p>The organization employs integrity verification tools to detect unauthorized changes to [Assignment: organization-defined software, firmware, and information].</p>	<p><a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a></p>	<p>Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.</p>

Control ID	Control Description	AWS Config Rule	Guidance
SI-7(1)	The information system performs an integrity check of [Assignment: organization-defined software, firmware, and information] [Selection (one or more): at startup; at [Assignment: organization-defined transitional states or security-relevant events]; [Assignment: organization- defined frequency]].	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
SI-7(1)	The information system performs an integrity check of [Assignment: organization-defined software, firmware, and information] [Selection (one or more): at startup; at [Assignment: organization-defined transitional states or security-relevant events]; [Assignment: organization- defined frequency]].	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.

Control ID	Control Description	AWS Config Rule	Guidance
SI-7(1)	The information system performs an integrity check of [Assignment: organization-defined software, firmware, and information] [Selection (one or more): at startup; at [Assignment: organization-defined transitional states or security-relevant events]; [Assignment: organization- defined frequency]].	<a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a>	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.
SI-12	The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.
SI-12	The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.

Control ID	Control Description	AWS Config Rule	Guidance
SI-12	The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.
SI-12	The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
SI-12	The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	<a href="#">rds-in-backup-plan (p. 167)</a>	To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	Control Description	AWS Config Rule	Guidance
SI-12	The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	<a href="#">ebs-in-backup-plan (p. 130)</a>	To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
SI-12	The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	<a href="#">efs-in-backup-plan (p. 139)</a>	To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
SI-12	The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	<a href="#">dynamodb-in-backup-plan (p. 128)</a>	To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	Control Description	AWS Config Rule	Guidance
SI-12	The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	<a href="#">cw-loggroup-retention-period-check (p. 125)</a>	Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events.

## Template

The template is available on GitHub: [Operational Best Practices for NIST 800-53 rev 4](#).

## Operational Best Practices for NIST 800 171

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the NIST 800-171 and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more NIST 800-171 controls. A NIST 800-171 control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This Conformance Pack was validated by AWS Security Assurance Services LLC (AWS SAS), which is a team of Payment Card Industry Qualified Security Assessors (QSAs), HITRUST Certified Common Security Framework Practitioners (CCSFPs), and compliance professionals certified to provide guidance and assessments for various industry frameworks. AWS SAS professionals designed this Conformance Pack to enable a customer to align to a subset of the NIST 800-171.

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
3.1.12	Monitor and control remote access sessions.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.12	Monitor and control remote access sessions.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
3.1.12	Monitor and control remote access sessions.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
3.1.12	Monitor and control remote access sessions.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.12	Monitor and control remote access sessions.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
3.1.12	Monitor and control remote access sessions.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
3.1.12	Monitor and control remote access sessions.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.12	Monitor and control remote access sessions.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
3.1.12	Monitor and control remote access sessions.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.12	Monitor and control remote access sessions.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
3.1.12	Monitor and control remote access sessions.	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
3.1.14	Route remote access via managed access control points.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.14	Route remote access via managed access control points.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
3.1.14	Route remote access via managed access control points.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
3.1.14	Route remote access via managed access control points.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
3.1.14	Route remote access via managed access control points.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.14	Route remote access via managed access control points.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
3.1.14	Route remote access via managed access control points.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.14	Route remote access via managed access control points.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
3.1.14	Route remote access via managed access control points.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
3.1.14	Route remote access via managed access control points.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.14	Route remote access via managed access control points.	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
3.1.14	Route remote access via managed access control points.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
3.1.14	Route remote access via managed access control points.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.14	Route remote access via managed access control points.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
3.1.14	Route remote access via managed access control points.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.14	Route remote access via managed access control points.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.
3.1.14	Route remote access via managed access control points.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
3.1.14	Route remote access via managed access control points.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.14	Route remote access via managed access control points.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
3.1.20	Verify and control/limit connections to and use of external systems.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.20	Verify and control/limit connections to and use of external systems.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
3.1.20	Verify and control/limit connections to and use of external systems.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.20	Verify and control/limit connections to and use of external systems.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
3.1.20	Verify and control/limit connections to and use of external systems.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling s3_bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.20	Verify and control/limit connections to and use of external systems.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
3.1.20	Verify and control/limit connections to and use of external systems.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
3.1.3	Control the flow of CUI in accordance with approved authorizations.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.3	Control the flow of CUI in accordance with approved authorizations.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
3.1.3	Control the flow of CUI in accordance with approved authorizations.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
3.1.3	Control the flow of CUI in accordance with approved authorizations.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
3.1.3	Control the flow of CUI in accordance with approved authorizations.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.3	Control the flow of CUI in accordance with approved authorizations.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
3.1.3	Control the flow of CUI in accordance with approved authorizations.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
3.1.3	Control the flow of CUI in accordance with approved authorizations.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.3	Control the flow of CUI in accordance with approved authorizations.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
3.1.3	Control the flow of CUI in accordance with approved authorizations.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
3.1.3	Control the flow of CUI in accordance with approved authorizations.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.3	Control the flow of CUI in accordance with approved authorizations.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
3.1.3	Control the flow of CUI in accordance with approved authorizations.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.3	Control the flow of CUI in accordance with approved authorizations.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
3.1.3	Control the flow of CUI in accordance with approved authorizations.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
3.1.3	Control the flow of CUI in accordance with approved authorizations.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.3	Control the flow of CUI in accordance with approved authorizations.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
3.1.3	Control the flow of CUI in accordance with approved authorizations.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
3.1.3	Control the flow of CUI in accordance with approved authorizations.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.6	Use non-privileged accounts or roles when accessing nonsecurity functions.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
3.1.7	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.7	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.
3.1.7	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
3.1.7	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.

Control ID	Control Description	AWS Config Rule	Guidance
3.1.7	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
3.1.7	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting the system are identified.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting the system are identified.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
3.11.3	Remediate vulnerabilities in accordance with assessments of risk.	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	<a href="#">alb-http-to-https-redirection-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	<a href="#">alb-waf-enabled (p. 109)</a>	Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.

Control ID	Control Description	AWS Config Rule	Guidance
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	<a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a>	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.

Control ID	Control Description	AWS Config Rule	Guidance
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.

Control ID	Control Description	AWS Config Rule	Guidance
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.

Control ID	Control Description	AWS Config Rule	Guidance
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.

Control ID	Control Description	AWS Config Rule	Guidance
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.

Control ID	Control Description	AWS Config Rule	Guidance
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.
3.13.10	Establish and manage cryptographic keys for cryptography employed in organizational systems.	<a href="#">cmk-backing-key-rotation-enabled (p. 123)</a>	Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period.

Control ID	Control Description	AWS Config Rule	Guidance
3.13.10	Establish and manage cryptographic keys for cryptography employed in organizational systems.	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.
3.13.16	Protect the confidentiality of CUI at rest.	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
3.13.16	Protect the confidentiality of CUI at rest.	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
3.13.16	Protect the confidentiality of CUI at rest.	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
3.13.16	Protect the confidentiality of CUI at rest.	<a href="#">dynamodb-table-encrypted-kms (p. 129)</a>	Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK).

Control ID	Control Description	AWS Config Rule	Guidance
3.13.16	Protect the confidentiality of CUI at rest.	<a href="#">ec2-ebs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
3.13.16	Protect the confidentiality of CUI at rest.	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
3.13.16	Protect the confidentiality of CUI at rest.	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
3.13.16	Protect the confidentiality of CUI at rest.	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
3.13.16	Protect the confidentiality of CUI at rest.	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.

Control ID	Control Description	AWS Config Rule	Guidance
3.13.16	Protect the confidentiality of CUI at rest.	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.
3.13.16	Protect the confidentiality of CUI at rest.	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.
3.13.16	Protect the confidentiality of CUI at rest.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
3.13.16	Protect the confidentiality of CUI at rest.	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.
3.13.16	Protect the confidentiality of CUI at rest.	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
3.13.16	Protect the confidentiality of CUI at rest.	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.
3.13.16	Protect the confidentiality of CUI at rest.	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
3.13.16	Protect the confidentiality of CUI at rest.	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">api-gw-endpoint-type-check (p. 110)</a>	Enable this rule to control Amazon API Gateway types allowed in your environment (edge optimized, regional API endpoints and Private API endpoints) and to ensure network integrity. This rule requires you to set an endpoint configuration type value (default: Regional). The actual value should reflect your organization's infrastructure type and applied policies.

Control ID	Control Description	AWS Config Rule	Guidance
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.

Control ID	Control Description	AWS Config Rule	Guidance
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.

Control ID	Control Description	AWS Config Rule	Guidance
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">cloudtrail-security-trail-enabled (p. 118)</a>	This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions.
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a>	The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.

Control ID	Control Description	AWS Config Rule	Guidance
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">dynamodb-autoscaling-enabled (p. 128)</a>	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.

Control ID	Control Description	AWS Config Rule	Guidance
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">dynamodb-throughput-limit-check (p. 130)</a>	Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set <code>accountRCUThresholdPercentage</code> (Config Default: 80) and <code>accountWCUThresholdPercentage</code> (Config Default: 80) parameters. The actual values should reflect your organization's policies.
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">ebs-optimized-instance (p. 131)</a>	An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance.

Control ID	Control Description	AWS Config Rule	Guidance
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">lambda-concurrency-check (p. 161)</a>	This rule ensures that a Lambda function's concurrency high and low limits are established. This can assist in baselining the number of requests that your function is serving at any given time.
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.

Control ID	Control Description	AWS Config Rule	Guidance
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">dynamodb-in-backup-plan (p. 128)</a>	To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">ebs-in-backup-plan (p. 130)</a>	To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	Control Description	AWS Config Rule	Guidance
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">efs-in-backup-plan (p. 139)</a>	To help with data backup processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a>	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">rds-instance-deletion-protection-enabled (p. 166)</a>	Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.

Control ID	Control Description	AWS Config Rule	Guidance
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	<a href="#">rds-in-backup-plan (p. 167)</a>	To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.

Control ID	Control Description	AWS Config Rule	Guidance
3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
3.14.1	Identify, report, and correct information and system flaws in a timely manner.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
3.14.1	Identify, report, and correct information and system flaws in a timely manner.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
3.14.2	Provide protection from malicious code at appropriate locations within organizational systems.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
3.14.2	Provide protection from malicious code at appropriate locations within organizational systems.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
3.14.3	Monitor system security alerts and advisories and take actions in response.	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.

Control ID	Control Description	AWS Config Rule	Guidance
3.14.3	Monitor system security alerts and advisories and take actions in response.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
3.14.3	Monitor system security alerts and advisories and take actions in response.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
3.14.4	Update malicious code protection mechanisms when new releases are available.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.
3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.

Control ID	Control Description	AWS Config Rule	Guidance
3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.
3.14.7	Identify unauthorized use of organizational systems.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.

Control ID	Control Description	AWS Config Rule	Guidance
3.14.7	Identify unauthorized use of organizational systems.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
3.14.7	Identify unauthorized use of organizational systems.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
3.14.7	Identify unauthorized use of organizational systems.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
3.14.7	Identify unauthorized use of organizational systems.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
3.14.7	Identify unauthorized use of organizational systems.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
3.14.7	Identify unauthorized use of organizational systems.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
3.14.7	Identify unauthorized use of organizational systems.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.

Control ID	Control Description	AWS Config Rule	Guidance
3.14.7	Identify unauthorized use of organizational systems.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
3.14.7	Identify unauthorized use of organizational systems.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
3.14.7	Identify unauthorized use of organizational systems.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
3.14.7	Identify unauthorized use of organizational systems.	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.
3.3.1	Create and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
3.3.1	Create and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
3.3.1	Create and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
3.3.1	Create and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
3.3.1	Create and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
3.3.1	Create and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
3.3.1	Create and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
3.3.1	Create and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.

Control ID	Control Description	AWS Config Rule	Guidance
3.3.1	Create and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
3.3.1	Create and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
3.3.1	Create and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
3.3.1	Create and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity.	<a href="#">cw-loggroup-retention-period-check (p. 125)</a>	Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events.
3.3.1	Create and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
3.3.1	Create and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity.	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.
3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	Control Description	AWS Config Rule	Guidance
3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
3.3.4	Alert in the event of an audit process failure.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
3.3.4	Alert in the event of an audit process failure.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
3.3.5	Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
3.3.5	Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
3.3.8	Protect audit information and audit tools from unauthorized access, modification, and deletion.	<a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a>	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.

Control ID	Control Description	AWS Config Rule	Guidance
3.3.8	Protect audit information and audit tools from unauthorized access, modification, and deletion.	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.
3.3.8	Protect audit information and audit tools from unauthorized access, modification, and deletion.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
3.3.8	Protect audit information and audit tools from unauthorized access, modification, and deletion.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
3.3.8	Protect audit information and audit tools from unauthorized access, modification, and deletion.	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
3.3.8	Protect audit information and audit tools from unauthorized access, modification, and deletion.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
3.3.8	Protect audit information and audit tools from unauthorized access, modification, and deletion.	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.
3.3.8	Protect audit information and audit tools from unauthorized access, modification, and deletion.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	<a href="#">ec2-security-group-attached-to-eni (p. 137)</a>	This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment.

Control ID	Control Description	AWS Config Rule	Guidance
3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	<a href="#">ec2-stopped-instance (p. 137)</a>	Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards.
3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	<a href="#">ec2-volume-in-use-check (p. 137)</a>	This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality.
3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	<a href="#">eip-attached (p. 139)</a>	This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment.
3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">ec2-volume-inuse-check (p. 137)</a>	This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality.

Control ID	Control Description	AWS Config Rule	Guidance
3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	Control Description	AWS Config Rule	Guidance
3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
3.4.7	Restrict, disable, and prevent the use of nonessential, functions, ports, protocols, or services.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
3.4.7	Restrict, disable, and prevent the use of nonessential, functions, ports, protocols, or services.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
3.4.7	Restrict, disable, and prevent the use of nonessential, functions, ports, protocols, or services.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
3.4.7	Restrict, disable, and prevent the use of nonessential, functions, ports, protocols, or services.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.

Control ID	Control Description	AWS Config Rule	Guidance
3.4.9	Control and monitor user-installed software.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
3.4.9	Control and monitor user-installed software.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
3.5.10	Store and transmit only cryptographically-protected passwords.	<a href="#">alb-http-to-https-redirection-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
3.5.10	Store and transmit only cryptographically-protected passwords.	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
3.5.10	Store and transmit only cryptographically-protected passwords.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
3.5.10	Store and transmit only cryptographically-protected passwords.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
3.5.10	Store and transmit only cryptographically-protected passwords.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
3.5.10	Store and transmit only cryptographically-protected passwords.	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
3.5.10	Store and transmit only cryptographically-protected passwords.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
3.5.10	Store and transmit only cryptographically-protected passwords.	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.

Control ID	Control Description	AWS Config Rule	Guidance
3.5.10	Store and transmit only cryptographically-protected passwords.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
3.5.10	Store and transmit only cryptographically-protected passwords.	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
3.5.2	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational systems.	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.

Control ID	Control Description	AWS Config Rule	Guidance
3.5.2	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational systems.	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.

Control ID	Control Description	AWS Config Rule	Guidance
3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	Control Description	AWS Config Rule	Guidance
3.5.5	Prevent reuse of identifiers for a defined period.	<a href="#">iam-password-policy (p. 154)</a>	The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
3.5.6	Disable identifiers after a defined period of inactivity.	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
3.5.6	Disable identifiers after a defined period of inactivity.	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.5.8	Prohibit password reuse for a specified number of generations.	<a href="#">iam-password-policy (p. 154)</a>	The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.
3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	<a href="#">lambda-dlq-check (p. 161)</a>	Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed.
3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

## Template

The template is available on GitHub: [Operational Best Practices for NIST 800 171](#).

## Operational Best Practices for NIST CSF

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the NIST Cyber Security Framework (CSF) and AWS managed Config rules. Each AWS Config rule applies to a specific AWS resource, and relates to one or more NIST CSF controls. A NIST CSF control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This Conformance Pack was validated by AWS Security Assurance Services LLC (AWS SAS), which is a team of Payment Card Industry Qualified Security Assessors (QSAs), HITRUST Certified Common Security Framework Practitioners (CCSFPs), and compliance professionals certified to provide guidance and assessments for various industry frameworks. AWS SAS professionals designed this Conformance Pack to enable you to align to a subset of the NIST CSF.

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

Control ID	Control Description	AWS Config Rule	Guidance
ID.AM-2	Software platforms and applications within the organization are inventoried	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
ID.AM-2	Software platforms and applications within the organization are inventoried	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration

Control ID	Control Description	AWS Config Rule	Guidance
			state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
ID.AM-3	Organizational communication and data flows are mapped	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
ID.AM-3	Organizational communication and data flows are mapped	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
ID.AM-3	Organizational communication and data flows are mapped	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
ID.AM-3	Organizational communication and data flows are mapped	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	<p>AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.</p>
ID.AM-3	Organizational communication and data flows are mapped	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	<p>To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
ID.AM-3	Organizational communication and data flows are mapped	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
ID.AM-3	Organizational communication and data flows are mapped	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
ID.BE-5	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	<a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a>	The ELB health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.
ID.BE-5	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.
ID.BE-5	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	<a href="#">dynamodb-autoscaling-enabled (p. 128)</a>	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.

Control ID	Control Description	AWS Config Rule	Guidance
ID.BE-5	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	<a href="#">dynamodb-throughput-limit-check (p. 130)</a>	Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account.
ID.BE-5	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
ID.BE-5	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.

Control ID	Control Description	AWS Config Rule	Guidance
ID.BE-5	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
ID.BE-5	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.

Control ID	Control Description	AWS Config Rule	Guidance
ID.BE-5	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.
ID.BE-5	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.
ID.RA-1	Asset vulnerabilities are identified and documented	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.

Control ID	Control Description	AWS Config Rule	Guidance
ID.RA-1	Asset vulnerabilities are identified and documented	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
ID.RA-1	Asset vulnerabilities are identified and documented	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
ID.RA-2	Threat and vulnerability information is received from information sharing forums and sources	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
ID.RA-2	Threat and vulnerability information is received from information sharing forums and sources	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
ID.RA-3	Threats, both internal and external, are identified and documented	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
ID.RA-3	Threats, both internal and external, are identified and documented	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	<a href="#">access-keys-rotated (p. 107)</a>	The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	Control Description	AWS Config Rule	Guidance
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.

Control ID	Control Description	AWS Config Rule	Guidance
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	<a href="#">secretsmanager-rotation-enabled-check (p. 183)</a>	This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised.
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	<a href="#">secretsmanager-scheduled-rotation-success-check (p. 184)</a>	This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised.
PR.AC-3	Remote access is managed	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
PR.AC-3	Remote access is managed	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
PR.AC-3	Remote access is managed	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
PR.AC-3	Remote access is managed	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
PR.AC-3	Remote access is managed	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
PR.AC-3	Remote access is managed	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
PR.AC-3	Remote access is managed	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
PR.AC-3	Remote access is managed	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
PR.AC-3	Remote access is managed	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
PR.AC-3	Remote access is managed	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
PR.AC-3	Remote access is managed	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
PR.AC-3	Remote access is managed	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
PR.AC-3	Remote access is managed	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
PR.AC-3	Remote access is managed	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
PR.AC-3	Remote access is managed	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
PR.AC-3	Remote access is managed	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
PR.AC-3	Remote access is managed	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	Control Description	AWS Config Rule	Guidance
PR.AC-3	Remote access is managed	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
PR.AC-3	Remote access is managed	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
PR.AC-3	Remote access is managed	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
PR.AC-3	Remote access is managed	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
PR.AC-3	Remote access is managed	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
PR.AC-3	Remote access is managed	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
PR.AC-3	Remote access is managed	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
PR.AC-3	Remote access is managed	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.

Control ID	Control Description	AWS Config Rule	Guidance
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	Control Description	AWS Config Rule	Guidance
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.

Control ID	Control Description	AWS Config Rule	Guidance
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.

Control ID	Control Description	AWS Config Rule	Guidance
PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.

Control ID	Control Description	AWS Config Rule	Guidance
PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.

Control ID	Control Description	AWS Config Rule	Guidance
PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	Control Description	AWS Config Rule	Guidance
PR.DS-1	Data-at-rest is protected	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
PR.DS-1	Data-at-rest is protected	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
PR.DS-1	Data-at-rest is protected	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
PR.DS-1	Data-at-rest is protected	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
PR.DS-1	Data-at-rest is protected	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
PR.DS-1	Data-at-rest is protected	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.

Control ID	Control Description	AWS Config Rule	Guidance
PR.DS-1	Data-at-rest is protected	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.
PR.DS-1	Data-at-rest is protected	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.
PR.DS-1	Data-at-rest is protected	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.
PR.DS-1	Data-at-rest is protected	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
PR.DS-1	Data-at-rest is protected	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.
PR.DS-1	Data-at-rest is protected	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.
PR.DS-1	Data-at-rest is protected	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.
PR.DS-2	Data-in-transit is protected	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
PR.DS-2	Data-in-transit is protected	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
PR.DS-2	Data-in-transit is protected	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
PR.DS-2	Data-in-transit is protected	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition	<a href="#">ec2-security-group-attached-to-eni (p. 137)</a>	This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment.

Control ID	Control Description	AWS Config Rule	Guidance
PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition	<a href="#">eip-attached (p. 139)</a>	This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment.
PR.DS-4	Adequate capacity to ensure availability is maintained	<a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a>	The ELB health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.
PR.DS-4	Adequate capacity to ensure availability is maintained	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.

Control ID	Control Description	AWS Config Rule	Guidance
PR.DS-4	Adequate capacity to ensure availability is maintained	<a href="#">dynamodb-throughput-limit-check (p. 130)</a>	Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account.
PR.DS-4	Adequate capacity to ensure availability is maintained	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
PR.DS-4	Adequate capacity to ensure availability is maintained	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.

Control ID	Control Description	AWS Config Rule	Guidance
PR.DS-4	Adequate capacity to ensure availability is maintained	<a href="#">rds-enhanced-monitoring-enabled (p. 165)</a>	Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics.

Control ID	Control Description	AWS Config Rule	Guidance
PR.DS-4	Adequate capacity to ensure availability is maintained	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
PR.DS-4	Adequate capacity to ensure availability is maintained	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.

Control ID	Control Description	AWS Config Rule	Guidance
PR.DS-4	Adequate capacity to ensure availability is maintained	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.
PR.DS-4	Adequate capacity to ensure availability is maintained	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.

Control ID	Control Description	AWS Config Rule	Guidance
PR.DS-5	Protections against data leaks are implemented	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
PR.DS-5	Protections against data leaks are implemented	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Amazon S3 data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
PR.DS-5	Protections against data leaks are implemented	<a href="#">codebuild-project-envvar-awscred-check (p. 123)</a>	Ensure authentication credentials <code>AWS_ACCESS_KEY_ID</code> and <code>AWS_SECRET_ACCESS_KEY</code> do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access.
PR.DS-5	Protections against data leaks are implemented	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
PR.DS-5	Protections against data leaks are implemented	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
PR.DS-5	Protections against data leaks are implemented	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
PR.DS-5	Protections against data leaks are implemented	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
PR.DS-5	Protections against data leaks are implemented	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
PR.DS-5	Protections against data leaks are implemented	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
PR.DS-5	Protections against data leaks are implemented	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
PR.DS-5	Protections against data leaks are implemented	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
PR.DS-5	Protections against data leaks are implemented	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
PR.DS-5	Protections against data leaks are implemented	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the <code>ignorePublicAcls</code> (Config Default: True), <code>blockPublicPolicy</code> (Config Default: True), <code>blockPublicAcls</code> (Config Default: True), and <code>restrictPublicBuckets</code> parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
PR.DS-5	Protections against data leaks are implemented	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
PR.DS-5	Protections against data leaks are implemented	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
PR.DS-5	Protections against data leaks are implemented	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
PR.DS-5	Protections against data leaks are implemented	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
PR.DS-5	Protections against data leaks are implemented	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
PR.DS-5	Protections against data leaks are implemented	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.

Control ID	Control Description	AWS Config Rule	Guidance
PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity	<a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a>	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.
PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	<a href="#">ec2-stopped-instance (p. 137)</a>	Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards.
PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	<a href="#">ec2-volume-inuse-check (p. 137)</a>	This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality.

Control ID	Control Description	AWS Config Rule	Guidance
PR.IP-3	Configuration change control processes are in place	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
PR.IP-4	Backups of information are conducted, maintained, and tested periodically	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.
PR.IP-4	Backups of information are conducted, maintained, and tested periodically	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.

Control ID	Control Description	AWS Config Rule	Guidance
PR.IP-4	Backups of information are conducted, maintained, and tested periodically	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
PR.IP-4	Backups of information are conducted, maintained, and tested periodically	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
PR.IP-4	Backups of information are conducted, maintained, and tested periodically	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.

Control ID	Control Description	AWS Config Rule	Guidance
PR.IP-7	Protection processes are improved	<a href="#">ebs-optimized-instance (p. 131)</a>	An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance.
PR.MA-2	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	Control Description	AWS Config Rule	Guidance
PR.MA-2	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
PR.PT-3	Access to systems and assets is controlled, incorporating the principle of least functionality	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
PR.PT-3	Access to systems and assets is controlled, incorporating the principle of least functionality	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
PR.PT-3	Access to systems and assets is controlled, incorporating the principle of least functionality	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
PR.PT-3	Access to systems and assets is controlled, incorporating the principle of least functionality	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
PR.PT-3	Access to systems and assets is controlled, incorporating the principle of least functionality	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	Control Description	AWS Config Rule	Guidance
PR.PT-3	Access to systems and assets is controlled, incorporating the principle of least functionality	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
PR.PT-3	Access to systems and assets is controlled, incorporating the principle of least functionality	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
PR.PT-3	Access to systems and assets is controlled, incorporating the principle of least functionality	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
PR.PT-3	Access to systems and assets is controlled, incorporating the principle of least functionality	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
PR.PT-3	Access to systems and assets is controlled, incorporating the principle of least functionality	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
PR.PT-3	Access to systems and assets is controlled, incorporating the principle of least functionality	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
PR.PT-4	Communications and control networks are protected	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
PR.PT-4	Communications and control networks are protected	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
PR.PT-4	Communications and control networks are protected	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the Amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.

Control ID	Control Description	AWS Config Rule	Guidance
PR.PT-4	Communications and control networks are protected	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
PR.PT-4	Communications and control networks are protected	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
PR.PT-4	Communications and control networks are protected	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
PR.PT-4	Communications and control networks are protected	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
PR.PT-4	Communications and control networks are protected	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.

Control ID	Control Description	AWS Config Rule	Guidance
PR.PT-5	Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	<a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a>	The ELB health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.
PR.PT-5	Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.
PR.PT-5	Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.

Control ID	Control Description	AWS Config Rule	Guidance
PR.PT-5	Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
PR.PT-5	Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.

Control ID	Control Description	AWS Config Rule	Guidance
PR.PT-5	Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
PR.PT-5	Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.
PR.PT-5	Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.

Control ID	Control Description	AWS Config Rule	Guidance
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed	<a href="#">lambda-concurrency-check (p. 161)</a>	This rule ensures that a Lambda function's concurrency high and low limits are established. This can assist in baselining the number of requests that your function is serving at any given time.
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.

Control ID	Control Description	AWS Config Rule	Guidance
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.

Control ID	Control Description	AWS Config Rule	Guidance
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
DE.AE-2	Detected events are analyzed to understand attack targets and methods	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
DE.AE-2	Detected events are analyzed to understand attack targets and methods	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
DE.AE-3	Event data are collected and correlated from multiple sources and sensors	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
DE.AE-3	Event data are collected and correlated from multiple sources and sensors	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
DE.AE-3	Event data are collected and correlated from multiple sources and sensors	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
DE.AE-3	Event data are collected and correlated from multiple sources and sensors	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Amazon S3 data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
DE.AE-3	Event data are collected and correlated from multiple sources and sensors	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
DE.AE-3	Event data are collected and correlated from multiple sources and sensors	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
DE.AE-3	Event data are collected and correlated from multiple sources and sensors	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
DE.AE-3	Event data are collected and correlated from multiple sources and sensors	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
DE.AE-3	Event data are collected and correlated from multiple sources and sensors	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
DE.AE-4	Impact of events is determined	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	Control Description	AWS Config Rule	Guidance
DE.AE-4	Impact of events is determined	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Amazon S3 data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
DE.AE-4	Impact of events is determined	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
DE.AE-4	Impact of events is determined	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
DE.AE-4	Impact of events is determined	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.
DE.AE-4	Impact of events is determined	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.

Control ID	Control Description	AWS Config Rule	Guidance
DE.AE-4	Impact of events is determined	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
DE.AE-4	Impact of events is determined	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
DE.AE-5	Incident alert thresholds are established	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
DE.AE-5	Incident alert thresholds are established	<a href="#">codebuild-project-source-repo-url-check (p. 123)</a>	Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, user name and password within AWS Codebuild project environments. Use OAuth instead of personal access tokens or a user name and password to grant authorization for accessing GitHub or Bitbucket repositories.
DE.AE-5	Incident alert thresholds are established	<a href="#">lambda-dlq-check (p. 161)</a>	Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed.

Control ID	Control Description	AWS Config Rule	Guidance
DE.CM-1	The network is monitored to detect potential cybersecurity events	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
DE.CM-1	The network is monitored to detect potential cybersecurity events	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
DE.CM-1	The network is monitored to detect potential cybersecurity events	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Amazon S3 data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
DE.CM-1	The network is monitored to detect potential cybersecurity events	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
DE.CM-1	The network is monitored to detect potential cybersecurity events	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
DE.CM-1	The network is monitored to detect potential cybersecurity events	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.

Control ID	Control Description	AWS Config Rule	Guidance
DE.CM-1	The network is monitored to detect potential cybersecurity events	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
DE.CM-1	The network is monitored to detect potential cybersecurity events	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
DE.CM-1	The network is monitored to detect potential cybersecurity events	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
DE.CM-3	Personnel activity is monitored to detect potential cybersecurity events	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
DE.CM-3	Personnel activity is monitored to detect potential cybersecurity events	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Amazon S3 data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.

Control ID	Control Description	AWS Config Rule	Guidance
DE.CM-3	Personnel activity is monitored to detect potential cybersecurity events	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
DE.CM-3	Personnel activity is monitored to detect potential cybersecurity events	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.

Control ID	Control Description	AWS Config Rule	Guidance
DE.CM-3	Personnel activity is monitored to detect potential cybersecurity events	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
DE.CM-3	Personnel activity is monitored to detect potential cybersecurity events	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
DE.CM-4	Malicious code is detected	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
DE.CM-4	Malicious code is detected	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
DE.CM-6	External service provider activity is monitored to detect potential cybersecurity events	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	Control Description	AWS Config Rule	Guidance
DE.CM-6	External service provider activity is monitored to detect potential cybersecurity events	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Amazon S3 data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
DE.CM-6	External service provider activity is monitored to detect potential cybersecurity events	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
DE.CM-6	External service provider activity is monitored to detect potential cybersecurity events	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.

Control ID	Control Description	AWS Config Rule	Guidance
DE.CM-6	External service provider activity is monitored to detect potential cybersecurity events	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
DE.CM-6	External service provider activity is monitored to detect potential cybersecurity events	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.

Control ID	Control Description	AWS Config Rule	Guidance
DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Amazon S3 data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.

Control ID	Control Description	AWS Config Rule	Guidance
DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
DE.DP-4	Event detection information is communicated	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
DE.DP-5	Detection processes are continuously improved	<a href="#">ec2-instance-detailed-monitoring-enabled (p. 132)</a>	Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance.

Control ID	Control Description	AWS Config Rule	Guidance
RS.AN-2	The impact of the incident is understood	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.

## Template

The template is available on GitHub: [Operational Best Practices for NIST CSF](#).

## Operational Best Practices for NYDFS 23

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the New York State Department Of Financial Services (NYDFS) cybersecurity requirements for financial services companies (23 NYCRR 500) and AWS managed Config rules. Each AWS Config rule applies to a specific AWS resource, and relates to one or more US NYDFS controls. A US NYDFS 23 NYCRR 500 control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This Conformance Pack was validated by AWS Security Assurance Services LLC (AWS SAS), which is a team of Payment Card Industry Qualified Security Assessors (QSAs), HITRUST Certified Common Security Framework Practitioners (CCSFPs), and compliance professionals certified to provide guidance and assessments for various industry frameworks. AWS SAS professionals designed this Conformance Pack to enable you to align to a subset of the US NYDFS 23 NYCRR 500 design principles.

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

Control ID	Control Description	AWS Config Rule	Guidance
500.02(a)	(a) Cybersecurity Program. Each Covered Entity shall maintain a	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509

Control ID	Control Description	AWS Config Rule	Guidance
	<p>cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.</p>		<p>certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.</p>
500.02(a)	<p>(a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.</p>	<p><a href="#">alb-http-to-https-redirect-check (p. 109)</a></p>	<p>To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.</p>
500.02(a)	<p>(a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.</p>	<p><a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a></p>	<p>To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.</p>
500.02(a)	<p>(a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.</p>	<p><a href="#">cloud-trail-encryption-enabled (p. 122)</a></p>	<p>Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.</p>
500.02(a)	<p>(a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.</p>	<p><a href="#">cloudwatch-log-group-encrypted (p. 121)</a></p>	<p>To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.</p>

Control ID	Control Description	AWS Config Rule	Guidance
500.02(a)	(a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
500.02(a)	(a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
500.02(a)	(a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
500.02(a)	(a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.

Control ID	Control Description	AWS Config Rule	Guidance
500.02(a)	(a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.
500.02(a)	(a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.
500.02(a)	(a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
500.02(a)	(a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
500.02(a)	(a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
500.02(a)	(a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.
500.02(a)	(a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
500.02(a)	(a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.
500.02(a)	(a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.	<a href="#">ec2-ebs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
500.02(a)	(a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.
500.02(a)	(a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
500.02(a)	(a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
500.02(a)	(a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
500.02(a)	(a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.	<a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a>	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.

Control ID	Control Description	AWS Config Rule	Guidance
500.02(a)	(a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.	<a href="#">dynamodb-autoscaling-enabled (p. 128)</a>	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.
500.02(a)	(a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.

Control ID	Control Description	AWS Config Rule	Guidance
500.02(a)	(a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
500.02(a)	(a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
500.02(a)	(a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.
500.02(a)	(a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.	<a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a>	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.
500.02(a)	(a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.	<a href="#">rds-instance-deletion-protection-enabled (p. 166)</a>	Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.

Control ID	Control Description	AWS Config Rule	Guidance
500.02(b)(2)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
500.02(b)(2)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	Control Description	AWS Config Rule	Guidance
500.02(b)(2)	<p>(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.</p>	<p><a href="#">iam-password-policy</a> (p. 154)</p>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
500.02(b)(2)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
500.02(b)(2)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.

Control ID	Control Description	AWS Config Rule	Guidance
500.02(b)(2)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
500.02(b)(2)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.

Control ID	Control Description	AWS Config Rule	Guidance
500.02(b)(2)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
500.02(b)(2)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
500.02(b)(2)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
500.02(b)(2)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	Control Description	AWS Config Rule	Guidance
500.02(b)(2)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
500.02(b)(2)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.	<a href="#">ec2-imdsv2-check (p. 132)</a>	Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata.

Control ID	Control Description	AWS Config Rule	Guidance
500.02(b)(2)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.
500.02(b)(2)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
500.02(b)(2)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
500.02(b)(2)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
500.02(b)(2)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
500.02(b)(2)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
500.02(b)(2)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
500.02(b)(2)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.

Control ID	Control Description	AWS Config Rule	Guidance
500.02(b)(2)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
500.02(b)(2)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
500.02(b)(2)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
500.02(b)(2)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
500.02(b)(2)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
500.02(b)(2)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
500.02(b)(2)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
500.02(b)(2)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
500.02(b)(2)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
500.02(b)(2)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
500.02(b)(2)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
500.02(b)(2)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	Control Description	AWS Config Rule	Guidance
500.02(b)(2)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
500.02(b)(2)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.	<a href="#">alb-waf-enabled (p. 109)</a>	Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.
500.02(b)(3)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (3) detect Cybersecurity Events.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
500.02(b)(3)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (3) detect Cybersecurity Events.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
500.02(b)(3)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (3) detect Cybersecurity Events.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
500.02(b)(3)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (3) detect Cybersecurity Events.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
500.02(b)(3)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (3) detect Cybersecurity Events.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
500.02(b)(3)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (3) detect Cybersecurity Events.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
500.02(b)(3)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (3) detect Cybersecurity Events.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
500.02(b)(3)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (3) detect Cybersecurity Events.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
500.02(b)(3)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (3) detect Cybersecurity Events.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
500.02(b)(3)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (3) detect Cybersecurity Events.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
500.02(b)(3)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (3) detect Cybersecurity Events.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
500.02(b)(3)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (3) detect Cybersecurity Events.	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.

Control ID	Control Description	AWS Config Rule	Guidance
500.02(b)(5)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (5) recover from Cybersecurity Events and restore normal operations and services.	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.
500.02(b)(5)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (5) recover from Cybersecurity Events and restore normal operations and services.	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.
500.02(b)(5)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (5) recover from Cybersecurity Events and restore normal operations and services.	<a href="#">ebs-optimized-instance (p. 131)</a>	An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance.

Control ID	Control Description	AWS Config Rule	Guidance
500.02(b)(5)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (5) recover from Cybersecurity Events and restore normal operations and services.	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
500.02(b)(5)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core functions: (5) recover from Cybersecurity Events and restore normal operations and services.	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
500.02(b)(5)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (5) recover from Cybersecurity Events and restore normal operations and services.	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.

Control ID	Control Description	AWS Config Rule	Guidance
500.02(b)(5)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (5) recover from Cybersecurity Events and restore normal operations and services.	<a href="#">dynamodb-in-backup-plan (p. 128)</a>	To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
500.02(b)(5)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (5) recover from Cybersecurity Events and restore normal operations and services.	<a href="#">ebs-in-backup-plan (p. 130)</a>	To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
500.02(b)(5)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (5) recover from Cybersecurity Events and restore normal operations and services.	<a href="#">efs-in-backup-plan (p. 139)</a>	To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	Control Description	AWS Config Rule	Guidance
500.02(b)(5)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (5) recover from Cybersecurity Events and restore normal operations and services.	<a href="#">rds-in-backup-plan (p. 167)</a>	To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
500.06(b)	(b) Each Covered Entity shall maintain records required by section 500.06(a)(1) of this Part for not fewer than five years and shall maintain records required by section 500.06(a)(2) of this Part for not fewer than three years.	<a href="#">cw-loggroup-retention-period-check (p. 125)</a>	Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events.
500.07	As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.	<a href="#">access-keys-rotated (p. 107)</a>	The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
500.07	As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.
500.07	As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.	<a href="#">secretsmanager-rotation-enabled-check (p. 183)</a>	This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised.
500.07	As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.	<a href="#">secretsmanager-scheduled-rotation-success-check (p. 184)</a>	This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised.

Control ID	Control Description	AWS Config Rule	Guidance
500.8(a)	(a) Each Covered Entity's cybersecurity program shall include written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications utilized by the Covered Entity, and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Covered Entity within the context of the Covered Entity's technology environment.	<a href="#">codebuild-project-envvar-awscred-check (p. 123)</a>	Ensure authentication credentials <code>AWS_ACCESS_KEY_ID</code> and <code>AWS_SECRET_ACCESS_KEY</code> do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access.
500.8(a)	(a) Each Covered Entity's cybersecurity program shall include written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications utilized by the Covered Entity, and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Covered Entity within the context of the Covered Entity's technology environment.	<a href="#">codebuild-project-source-repo-url-check (p. 123)</a>	Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, user name and password within AWS Codebuild project environments. Use OAuth instead of personal access tokens or a user name and password to grant authorization for accessing GitHub or Bitbucket repositories.

Control ID	Control Description	AWS Config Rule	Guidance
500.14(a)	(a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users.	<a href="#">cloudwatch-alarm-action-check (p. 119)</a>	Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for <code>alarmActionRequired</code> (Config Default: True), <code>insufficientDataActionRequired</code> (Config Default: True), <code>okActionRequired</code> (Config Default: False). The actual value should reflect the alarm actions for your environment.
500.02(b)(3)	(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (3) detect Cybersecurity Events.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
500.06(a)	(a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment: (1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and (2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
500.06(a)	(a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment: (1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and (2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.

Control ID	Control Description	AWS Config Rule	Guidance
500.06(a)	(a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment: (1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and (2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
500.06(a)	(a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment: (1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and (2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.

Control ID	Control Description	AWS Config Rule	Guidance
500.06(a)	(a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment: (1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and (2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
500.06(a)	(a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment: (1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and (2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.

Control ID	Control Description	AWS Config Rule	Guidance
500.06(a)	(a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment: (1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and (2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
500.06(a)	(a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment: (1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and (2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.

Control ID	Control Description	AWS Config Rule	Guidance
500.06(a)	(a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment: (1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and (2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.
500.06(a)	(a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment: (1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and (2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity.	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.

Control ID	Control Description	AWS Config Rule	Guidance
500.06(a)	(a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment: (1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and (2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
500.07	As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
500.07	As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	Control Description	AWS Config Rule	Guidance
500.07	<p>As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.</p>	<p><a href="#">iam-password-policy (p. 154)</a></p>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
500.07	As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
500.07	As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
500.07	As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
500.07	As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
500.07	As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
500.07	As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.

Control ID	Control Description	AWS Config Rule	Guidance
500.07	As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
500.07	As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
500.07	As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
500.07	As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
500.07	As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
500.07	As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
500.07	As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.

Control ID	Control Description	AWS Config Rule	Guidance
500.07	As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
500.07	As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
500.07	As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
500.07	As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
500.07	As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
500.07	As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
500.07	As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
500.07	As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
500.07	As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.

Control ID	Control Description	AWS Config Rule	Guidance
500.12	<p>(a) Multi-Factor Authentication. Based on its Risk Assessment, each Covered Entity shall use effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to Nonpublic Information or Information Systems.</p> <p>(b) Multi-Factor Authentication shall be utilized for any individual accessing the Covered Entity's internal networks from an external network, unless the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls.</p>	<a href="#">iam-user-mfa-enabled (p. 158)</a>	<p>Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.</p>
500.12	<p>(a) Multi-Factor Authentication. Based on its Risk Assessment, each Covered Entity shall use effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to Nonpublic Information or Information Systems.</p> <p>(b) Multi-Factor Authentication shall be utilized for any individual accessing the Covered Entity's internal networks from an external network, unless the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls.</p>	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	<p>Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.</p>

Control ID	Control Description	AWS Config Rule	Guidance
500.12	<p>(a) Multi-Factor Authentication. Based on its Risk Assessment, each Covered Entity shall use effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to Nonpublic Information or Information Systems.</p> <p>(b) Multi-Factor Authentication shall be utilized for any individual accessing the Covered Entity's internal networks from an external network, unless the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls.</p>	<a href="#">iam-root-access-key-check (p. 157)</a>	<p>Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.</p>
500.12	<p>(a) Multi-Factor Authentication. Based on its Risk Assessment, each Covered Entity shall use effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to Nonpublic Information or Information Systems.</p> <p>(b) Multi-Factor Authentication shall be utilized for any individual accessing the Covered Entity's internal networks from an external network, unless the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls.</p>	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	<p>Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.</p>

Control ID	Control Description	AWS Config Rule	Guidance
500.12	<p>(a) Multi-Factor Authentication. Based on its Risk Assessment, each Covered Entity shall use effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to Nonpublic Information or Information Systems.</p> <p>(b) Multi-Factor Authentication shall be utilized for any individual accessing the Covered Entity's internal networks from an external network, unless the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls.</p>	<a href="#">root-account-mfa-enabled (p. 175)</a>	<p>Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.</p>
500.14(a)	<p>(a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users.</p>	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	<p>API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.</p>
500.14(a)	<p>(a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users.</p>	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	<p>Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.</p>

Control ID	Control Description	AWS Config Rule	Guidance
500.14(a)	(a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
500.14(a)	(a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
500.14(a)	(a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
500.14(a)	(a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users.	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.
500.14(a)	(a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
500.14(a)	(a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
500.14(a)	(a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users.	<a href="#">cw-loggroup-retention-period-check (p. 125)</a>	Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events.
500.14(a)	(a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users.	<a href="#">rds-logging-enabled (p. 167)</a>	To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.

Control ID	Control Description	AWS Config Rule	Guidance
500.14(a)	(a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users.	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.
500.14(a)	(a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
500.14(a)	(a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
500.14(a)	(a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.
500.15(a)	(a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.
500.15(a)	(a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
500.15(a)	(a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
500.15(a)	(a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
500.15(a)	(a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
500.15(a)	(a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).

Control ID	Control Description	AWS Config Rule	Guidance
500.15(a)	(a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
500.15(a)	(a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
500.15(a)	(a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
500.15(a)	(a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
500.15(a)	(a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
500.15(a)	(a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
500.15(a)	(a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
500.15(a)	(a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
500.15(a)	(a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.
500.15(a)	(a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
500.15(a)	(a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.
500.15(a)	(a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.	<a href="#">ec2-ebs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
500.15(a)	(a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
500.15(a)	(a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
500.15(a)	(a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
500.15(a)	(a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.

## Template

The template is available on GitHub: [Operational Best Practices for NYDFS 23](#).

## Operational Best Practices for PCI DSS 3.2.1

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Payment Card Data Security Standard (PCI DSS) 3.2.1 and AWS managed Config rules. Each AWS Config rule applies to a specific AWS resource, and relates to one or more PCI DSS controls. A PCI DSS control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This Conformance Pack was validated by AWS Security Assurance Services LLC (AWS SAS), which is a team of Payment Card Industry Qualified Security Assessors (QSAs), HITRUST Certified Common Security Framework Practitioners (CSFPs), and compliance professionals certified to provide guidance and assessments for various industry frameworks. AWS SAS professionals designed this Conformance Pack to enable a customer to align to a subset of the PCI DSS.

**AWS Region:** All supported AWS Regions except Asia Pacific (Hong Kong), Europe (Stockholm), and Middle East (Bahrain)

Control ID	Control Description	AWS Config Rule	Guidance
1.2	Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC

Control ID	Control Description	AWS Config Rule	Guidance
			without the need for an internet gateway, NAT device, or VPN connection.
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.

Control ID	Control Description	AWS Config Rule	Guidance
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.

Control ID	Control Description	AWS Config Rule	Guidance
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.

Control ID	Control Description	AWS Config Rule	Guidance
2.1	Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
2.2	Develop configuration standards for all system components.	<a href="#">eip-attached (p. 139)</a>	This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment.
2.2	Develop configuration standards for all system components.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.

Control ID	Control Description	AWS Config Rule	Guidance
2.4	Maintain an inventory of system components that are in scope for PCI DSS.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
2.4	Maintain an inventory of system components that are in scope for PCI DSS.	<a href="#">ec2-security-group-attached-to-eni (p. 137)</a>	This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment.
3.4	Render PAN unreadable anywhere it is stored.	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
3.4	Render PAN unreadable anywhere it is stored.	<a href="#">dynamodb-table-encryption-enabled (p. 129)</a>	Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK).
3.4	Render PAN unreadable anywhere it is stored.	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).
3.4	Render PAN unreadable anywhere it is stored.	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
3.4	Render PAN unreadable anywhere it is stored.	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
3.4	Render PAN unreadable anywhere it is stored.	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
3.4	Render PAN unreadable anywhere it is stored.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (PCI DSS Default : TRUE), and <code>loggingEnabled</code> (PCI DSS Default: TRUE). The actual values should reflect your organization's policies.
3.4	Render PAN unreadable anywhere it is stored.	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.
3.4	Render PAN unreadable anywhere it is stored.	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
3.4	Render PAN unreadable anywhere it is stored.	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.
3.6.4	Cryptographic key changes for keys that have reached the end of their cryptoperiod.	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.
3.6.4	Cryptographic key changes for keys that have reached the end of their cryptoperiod.	<a href="#">cmk-backing-key-rotation-enabled (p. 123)</a>	Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period.
4.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks.	<a href="#">alb-http-to-https-redirect-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
4.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks.	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
4.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks.	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
4.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks.	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
6.1	Establish a process to identify security vulnerabilities.	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.

Control ID	Control Description	AWS Config Rule	Guidance
6.2	Ensure that all system components and software are protected from known vulnerabilities.	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
7.1	Limit access to system components and cardholder data to only those individuals whose job requires such access.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
7.1.2	Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	Control Description	AWS Config Rule	Guidance
7.2	Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
7.2	Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
7.2	Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	Control Description	AWS Config Rule	Guidance
7.2	Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
7.2	Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
7.2	Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
7.2	Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
7.2	Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.
7.2	Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
7.2	Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
8.1.4	Remove/disable inactive user accounts within 90 days.	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (PCI DSS Default: 90). The actual value should reflect your organization's policies.
8.2.1	Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	<a href="#">codebuild-project-envvar-awscred-check (p. 123)</a>	Ensure authentication credentials <code>AWS_ACCESS_KEY_ID</code> and <code>AWS_SECRET_ACCESS_KEY</code> do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access.
8.2.1	Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	<a href="#">codebuild-project-source-repo-url-check (p. 123)</a>	Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, user name and password within AWS Codebuild project environments. Use OAuth instead of personal access tokens or a user name and password to grant authorization for accessing GitHub or Bitbucket repositories.

Control ID	Control Description	AWS Config Rule	Guidance
8.2.1	Using strong cryptography, render all authentication credentials unreadable during transmission and storage on all system components.	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.

Control ID	Control Description	AWS Config Rule	Guidance
8.2.3	Passwords/passphrases must meet the following: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters.	<a href="#">iam-password-policy (p. 154)</a>	The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (PCI DSS Default: false), <code>RequireLowercaseCharacters</code> (PCI DSS Default: true), <code>RequireSymbols</code> (PCI DSS Default: false), <code>RequireNumbers</code> (PCI DSS Default: true), <code>MinimumPasswordLength</code> (PCI DSS Default: 7), <code>PasswordReusePrevention</code> (PCI DSS Default: 4), and <code>MaxPasswordAge</code> (PCI DSS Default: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
8.2.4	Change user passwords/passphrases at least once every 90 days.	<a href="#">access-keys-rotated (p. 107)</a>	The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (PCI DSS Default: 90). The actual value should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
8.2.4	Change user passwords/passphrases at least once every 90 days.	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (PCI DSS Default: false), <code>RequireLowercaseCharacters</code> (PCI DSS Default: true), <code>RequireSymbols</code> (PCI DSS Default: false), <code>RequireNumbers</code> (PCI DSS Default: true), <code>MinimumPasswordLength</code> (PCI DSS Default: 7), <code>PasswordReusePrevention</code> (PCI DSS Default: 4), and <code>MaxPasswordAge</code> (PCI DSS Default: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>
8.2.4	Change user passwords/passphrases at least every 90 days.	<a href="#">secretsmanager-rotation-enabled-check (p. 183)</a>	<p>This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised.</p>

Control ID	Control Description	AWS Config Rule	Guidance
8.2.5	Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.	<a href="#">iam-password-policy (p. 154)</a>	The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (PCI DSS Default: false), <code>RequireLowercaseCharacters</code> (PCI DSS Default: true), <code>RequireSymbols</code> (PCI DSS Default: false), <code>RequireNumbers</code> (PCI DSS Default: true), <code>MinimumPasswordLength</code> (PCI DSS Default: 7), <code>PasswordReusePrevention</code> (PCI DSS Default: 4), and <code>MaxPasswordAge</code> (PCI DSS Default: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.
8.3	Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.

Control ID	Control Description	AWS Config Rule	Guidance
8.3	Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
8.3	Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
8.3	Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication..	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	Control Description	AWS Config Rule	Guidance
10.1	Implement audit trails to link all access to system components to each individual user.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (PCI DSS Default : TRUE), and <code>loggingEnabled</code> (PCI DSS Default: TRUE). The actual values should reflect your organization's policies.
10.1	Implement audit trails to link all access to system components to each individual user.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
10.2	Implement automated audit trails for all system components.	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
10.2	Implement automated audit trails for all system components.	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
10.2	Implement automated audit trails for all system components.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (PCI DSS Default : TRUE), and <code>loggingEnabled</code> (PCI DSS Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
10.2.1	Implement automated audit trails for all system components to reconstruct the all individual user accesses to cardholder data.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
10.2.1	Implement automated audit trails for all system components to reconstruct the all individual user accesses to cardholder data.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (PCI DSS Default : TRUE), and loggingEnabled (PCI DSS Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
10.2.1	Implement automated audit trails for all system components to reconstruct the all individual user accesses to cardholder data.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
10.2.2	Implement automated audit trails for all system components to reconstruct the all actions taken by any individual with root or administrative privileges.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	Control Description	AWS Config Rule	Guidance
10.2.2	Implement automated audit trails for all system components to reconstruct the all actions taken by any individual with root or administrative privileges.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (PCI DSS Default : TRUE), and loggingEnabled (PCI DSS Default: TRUE). The actual values should reflect your organization's policies.
10.2.2	Implement automated audit trails for all system components to reconstruct the all actions taken by any individual with root or administrative privileges.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
10.2.3	Implement automated audit trails for all system components to reconstruct the access to all audit trails.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
10.2.3	Implement automated audit trails for all system components to reconstruct the access to all audit trails.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
10.2.4	Implement automated audit trails for all system components to reconstruct the invalid logical access attempts.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	Control Description	AWS Config Rule	Guidance
10.2.4	Implement automated audit trails for all system components to reconstruct the invalid logical access attempts.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (PCI DSS Default : TRUE), and <code>loggingEnabled</code> (PCI DSS Default: TRUE). The actual values should reflect your organization's policies.
10.2.4	Implement automated audit trails for all system components to reconstruct the invalid logical access attempts.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
10.2.5	Implement automated audit trails for all system components to reconstruct the use of and changes to identification and authentication mechanisms.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
10.2.5	Implement automated audit trails for all system components to reconstruct the use of and changes to identification and authentication mechanisms.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (PCI DSS Default : TRUE), and loggingEnabled (PCI DSS Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
10.2.6	Implement automated audit trails for all system components to reconstruct the initialization, stopping, or pausing of the audit logs.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
10.2.7	Implement automated audit trails for all system components to reconstruct the creation and deletion of system-level objects.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
10.2.7	Implement automated audit trails for all system components to reconstruct the creation and deletion of system-level objects.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
10.3.1	Record within audit entries for all system components the user identification.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
10.3.1	Record within audit entries for all system components the user identification.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Amazon S3 data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
10.3.1	Record within audit entries for all system components the user identification.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
10.3.1	Record within audit entries for all system components the user identification.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (PCI DSS Default : TRUE), and loggingEnabled (PCI DSS Default: TRUE). The actual values should reflect your organization's policies.
10.3.1	Record within audit entries for all system components the user identification.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
10.3.2	Record within audit entries for all system components the type of event.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
10.3.2	Record within audit entries for all system components the type of event.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Amazon S3 data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
10.3.2	Record within audit entries for all system components the type of event.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
10.3.2	Record within audit entries for all system components the type of event.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (PCI DSS Default : TRUE), and <code>loggingEnabled</code> (PCI DSS Default: TRUE). The actual values should reflect your organization's policies.
10.3.2	Record within audit entries for all system components the type of event.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
10.3.3	Record within audit entries for all system components the date and time.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
10.3.3	Record within audit entries for all system components the date and time.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Amazon S3 data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
10.3.3	Record within audit entries for all system components the date and time.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
10.3.3	Record within audit entries for all system components the date and time.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (PCI DSS Default : TRUE), and <code>loggingEnabled</code> (PCI DSS Default: TRUE). The actual values should reflect your organization's policies.
10.3.3	Record within audit entries for all system components the date and time.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.

Control ID	Control Description	AWS Config Rule	Guidance
10.3.3	Record within audit entries for all system components the date and time.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
10.3.4	Record within audit entries for all system components the success or failure indication.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
10.3.4	Record within audit entries for all system components the success or failure indication.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Amazon S3 data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.

Control ID	Control Description	AWS Config Rule	Guidance
10.3.4	Record within audit entries for all system components the success or failure indication.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
10.3.4	Record within audit entries for all system components the success or failure indication.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (PCI DSS Default : TRUE), and loggingEnabled (PCI DSS Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
10.3.4	Record within audit entries for all system components the success or failure indication.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
10.3.4	Record within audit entries for all system components the success or failure indication.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
10.3.5	Record within audit entries for all system components the origination of event.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	Control Description	AWS Config Rule	Guidance
10.3.5	Record within audit entries for all system components the origination of event.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Amazon S3 data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
10.3.5	Record within audit entries for all system components the origination of event.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
10.3.5	Record within audit entries for all system components the origination of event.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (PCI DSS Default : TRUE), and loggingEnabled (PCI DSS Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
10.3.5	Record within audit entries for all system components the origination of event.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
10.3.5	Record within audit entries for all system components the origination of event.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
10.3.6	Record within audit entries for all system components the identity or name of affected data, system component, or resource.	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	Control Description	AWS Config Rule	Guidance
10.3.6	Record within audit entries for all system components the identity or name of affected data, system component, or resource.	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Amazon S3 data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
10.3.6	Record within audit entries for all system components the identity or name of affected data, system component, or resource.	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
10.3.6	Record within audit entries for all system components the identity or name of affected data, system component, or resource.	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (PCI DSS Default : TRUE), and loggingEnabled (PCI DSS Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
10.3.6	Record within audit entries for all system components the identity or name of affected data, system component, or resource.	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
10.3.6	Record within audit entries for all system components the identity or name of affected data, system component, or resource.	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
10.5.1	Limit viewing of audit trails to those with a job-related need.	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
10.5.1	Limit viewing of audit trails to those with a job-related need.	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.

Control ID	Control Description	AWS Config Rule	Guidance
10.5.2	Protect audit trail files from unauthorized modifications.	<a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a>	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.
10.5.3	Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.

Control ID	Control Description	AWS Config Rule	Guidance
10.5.5	Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts.	<a href="#">cloud-trail-log-file-validation-enabled (p. 122)</a>	Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.
10.6	Review logs and security events for all system components to identify anomalies or suspicious activity.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
11.4	Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
12.5.2	Monitor and analyze security alerts and information, and distribute to appropriate personnel.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

## Template

The template is available on GitHub: [Operational Best Practices for PCI DSS 3.2.1](#).

# Operational Best Practices for Publicly Accessible Resources

This conformance pack helps identify resources that may be publicly accessible.

This Conformance Pack has been designed for compatibility with the majority of AWS regions and to not require setting of any Parameters. Additional managed rules that require parameters to be set for your environment and/or for your specific region can be found at: [List of AWS Config Managed Rules](#).

**AWS Region:** All supported AWS Regions except Asia Pacific (Hong Kong), Europe (Stockholm), and Middle East (Bahrain)

See Parameters section for names and descriptions of required parameters.

The template is available on GitHub: [Operational Best Practices for Publicly Accessible Resources](#).

## Operational Best Practices for RBI Cyber Security Framework for UCBs

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Reserve Bank of India (RBI) Cyber Security Framework for Urban Cooperative Banks (UCBs) and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more RBI Cyber Security Framework for UCBs controls. An RBI Cyber Security Framework for UCBs control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

Control ID	AWS Config Rule	Guidance
Annex_I(1.1)	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
Annex_I(1.3)	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.
Annex_I(1.3)	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.

Control ID	AWS Config Rule	Guidance
Annex_I(1.3)	<a href="#">alb-http-to-https-redirection-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
Annex_I(1.3)	<a href="#">api-gw-cache-enabled-and-encrypted (p. 110)</a>	To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data.
Annex_I(1.3)	<a href="#">cloud-trail-encryption-enabled (p. 122)</a>	Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails.
Annex_I(1.3)	<a href="#">cloudwatch-log-group-encrypted (p. 121)</a>	To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups.
Annex_I(1.3)	<a href="#">cmk-backing-key-rotation-enabled (p. 123)</a>	Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period.
Annex_I(1.3)	<a href="#">dynamodb-table-encrypted-kms (p. 129)</a>	Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK).
Annex_I(1.3)	<a href="#">ec2-efs-encryption-by-default (p. 131)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data.
Annex_I(1.3)	<a href="#">efs-encrypted-check (p. 138)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS).

Control ID	AWS Config Rule	Guidance
Annex_I(1.3)	<a href="#">elasticsearch-encrypted-at-rest (p. 141)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains.
Annex_I(1.3)	<a href="#">elasticsearch-node-to-node-encryption-check (p. 142)</a>	Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data.
Annex_I(1.3)	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.
Annex_I(1.3)	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
Annex_I(1.3)	<a href="#">encrypted-volumes (p. 146)</a>	Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes.
Annex_I(1.3)	<a href="#">kms-cmk-not-scheduled-for-deletion (p. 160)</a>	To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally.

Control ID	AWS Config Rule	Guidance
Annex_I(1.3)	<a href="#">rds-snapshot-encrypted (p. 168)</a>	Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data.
Annex_I(1.3)	<a href="#">rds-storage-encrypted (p. 169)</a>	To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data.
Annex_I(1.3)	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.
Annex_I(1.3)	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
Annex_I(1.3)	<a href="#">s3-bucket-server-side-encryption-enabled (p. 181)</a>	To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data.

Control ID	AWS Config Rule	Guidance
Annex_I(1.3)	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
Annex_I(1.3)	<a href="#">sagemaker-endpoint-configuration-kms-key-configured (p. 182)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data.
Annex_I(1.3)	<a href="#">sagemaker-notebook-instance-kms-key-configured (p. 183)</a>	To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data.
Annex_I(1.3)	<a href="#">sns-encrypted-kms (p. 187)</a>	To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data.
Annex_I(1.3)	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
Annex_I(1.3)	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
Annex_I(1.3)	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
Annex_I(1.3)	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.
Annex_I(1.3)	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
Annex_I(1.3)	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.

Control ID	AWS Config Rule	Guidance
Annex_I(1.3)	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
Annex_I(1.3)	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.
Annex_I(1.3)	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
Annex_I(1.3)	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.

Control ID	AWS Config Rule	Guidance
Annex_I(1.3)	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
Annex_I(1.3)	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
Annex_I(1.3)	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.
Annex_I(1.3)	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
Annex_I(1.3)	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
Annex_I(1.3)	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
Annex_I(1.3)	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
Annex_I(5.1)	<a href="#">alb-waf-enabled (p. 109)</a>	Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.
Annex_I(5.1)	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.

Control ID	AWS Config Rule	Guidance
Annex_I(5.1)	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.
Annex_I(6)	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
Annex_I(6)	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
Annex_I(6)	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies.

Control ID	AWS Config Rule	Guidance
Annex_I(7.1)	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
Annex_I(7.1)	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
Annex_I(7.1)	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
Annex_I(7.1)	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.

Control ID	AWS Config Rule	Guidance
Annex_I(7.2)	<a href="#">iam-password-policy (p. 154)</a>	The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.
Annex_I(7.3)	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.
Annex_I(7.4)	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.

Control ID	AWS Config Rule	Guidance
Annex_I(7.4)	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
Annex_I(7.4)	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.
Annex_I(7.4)	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
Annex_I(7.4)	<a href="#">cw-loggroup-retention-period-check (p. 125)</a>	Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events.
Annex_I(7.4)	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	AWS Config Rule	Guidance
Annex_I(7.4)	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	<p>AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.</p>
Annex_I(7.4)	<a href="#">rds-logging-enabled (p. 167)</a>	<p>To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.</p>
Annex_I(7.4)	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	<p>Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.</p>

Control ID	AWS Config Rule	Guidance
Annex_I(7.4)	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.
Annex_I(7.4)	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.
Annex_I(7.4)	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for <code>clusterDbEncrypted</code> (Config Default : TRUE), and <code>loggingEnabled</code> (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	AWS Config Rule	Guidance
Annex_I(12)	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.
Annex_I(12)	<a href="#">dynamodb-in-backup-plan (p. 128)</a>	To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
Annex_I(12)	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.
Annex_I(12)	<a href="#">ebs-in-backup-plan (p. 130)</a>	To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	AWS Config Rule	Guidance
Annex_I(12)	<a href="#">efs-in-backup-plan (p. 139)</a>	To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
Annex_I(12)	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
Annex_I(12)	<a href="#">rds-in-backup-plan (p. 167)</a>	To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
Annex_I(12)	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.

Control ID	AWS Config Rule	Guidance
Annex_I(12)	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.

## Template

The template is available on GitHub: [Operational Best Practices for RBI Cyber Security Framework for UCBs](#).

## Operational Best Practices for RBI MD-ITF

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Reserve Bank of India (RBI) Master Direction – Information Technology Framework and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more RBI Master Direction – Information Technology Framework controls. An RBI Master Direction – Information Technology Framework control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

Control ID	Control Description	AWS Config Rule	Guidance
3.1(a)	Identification and Classification of Information Assets.	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type,

Control ID	Control Description	AWS Config Rule	Guidance
			software installations, application name, publisher and version, and other details about your environment.
3.1(c)	Role Based Access Control	<a href="#">access-keys-rotated (p. 107)</a>	The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
3.1(c)	Role Based Access Control	<a href="#">emr-kerberos-enabled (p. 145)</a>	<p>The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.</p>
3.1(c)	Role Based Access Control	<a href="#">iam-group-has-users-check (p. 153)</a>	<p>AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1(c)	Role Based Access Control	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.

Control ID	Control Description	AWS Config Rule	Guidance
3.1(c)	Role Based Access Control	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1(c)	Role Based Access Control	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
3.1(c)	Role Based Access Control	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
3.1(c)	Role Based Access Control	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
3.1(c)	Role Based Access Control	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
3.1(c)	Role Based Access Control	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
3.1(c)	Role Based Access Control	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
3.1(c)	Role Based Access Control	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
3.1(c)	Role Based Access Control	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
3.1(c)	Role Based Access Control	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	Control Description	AWS Config Rule	Guidance
3.1(c)	Role Based Access Control	<a href="#">secretsmanager-rotation-enabled-check (p. 183)</a>	This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised.
3.1(c)	Role Based Access Control	<a href="#">secretsmanager-scheduled-rotation-success-check (p. 184)</a>	This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised.
3.1(g)	Incident Management	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
3.1(g)	Incident Management	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
3.1(g)	Incident Management	<a href="#">alb-waf-enabled (p. 109)</a>	Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment.
3.1(g)	Incident Management	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

Control ID	Control Description	AWS Config Rule	Guidance
3.1(g)	Incident Management	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.
3.1(h)	Trails	<a href="#">api-gw-execution-logging-enabled (p. 111)</a>	API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities.
3.1(h)	Trails	<a href="#">cloud-trail-cloud-watch-logs-enabled (p. 121)</a>	Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account.
3.1(h)	Trails	<a href="#">cloudtrail-enabled (p. 121)</a>	AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents.

Control ID	Control Description	AWS Config Rule	Guidance
3.1(h)	Trails	<a href="#">cloudtrail-s3-dataevents-enabled (p. 118)</a>	The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event.
3.1(h)	Trails	<a href="#">cw-loggroup-retention-period-check (p. 125)</a>	Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events.
3.1(h)	Trails	<a href="#">elb-logging-enabled (p. 144)</a>	Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses.

Control ID	Control Description	AWS Config Rule	Guidance
3.1(h)	Trails	<a href="#">multi-region-cloudtrail-enabled (p. 163)</a>	<p>AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if <code>MULTI_REGION_CLOUD_TRAIL_ENABLED</code> is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action.</p>
3.1(h)	Trails	<a href="#">rds-logging-enabled (p. 167)</a>	<p>To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried.</p>

Control ID	Control Description	AWS Config Rule	Guidance
3.1(h)	Trails	<a href="#">s3-bucket-logging-enabled (p. 177)</a>	Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant.
3.1(h)	Trails	<a href="#">vpc-flow-logs-enabled (p. 188)</a>	The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol.

Control ID	Control Description	AWS Config Rule	Guidance
3.1(h)	Trails	<a href="#">wafv2-logging-enabled (p. 190)</a>	To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched.
3.1(h)	Trails	<a href="#">redshift-cluster-configuration-check (p. 170)</a>	To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
3.1(i)	Public Key Infrastructure	<a href="#">acm-certificate-expiration-check (p. 108)</a>	Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies.
3.1_i	Public Key Infrastructure	<a href="#">alb-http-drop-invalid-header-enabled (p. 109)</a>	Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data.
3.1(i)	Public Key Infrastructure	<a href="#">alb-http-to-https-redirection-check (p. 109)</a>	To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data.
3.1(i)	Public Key Infrastructure	<a href="#">elb-acm-certificate-required (p. 143)</a>	Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources.

Control ID	Control Description	AWS Config Rule	Guidance
3.1(i)	Public Key Infrastructure	<a href="#">elb-tls-https-listeners-only (p. 145)</a>	Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data.
3.1(i)	Public Key Infrastructure	<a href="#">redshift-require-tls-ssl (p. 172)</a>	Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data.
3.1(i)	Public Key Infrastructure	<a href="#">s3-bucket-ssl-requests-only (p. 181)</a>	To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data.
3.3	Vulnerability Management	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
3.3	Vulnerability Management	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
3.3	Vulnerability Management	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
3.3	Vulnerability Management	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.

Control ID	Control Description	AWS Config Rule	Guidance
3.5	Cyber Crisis Management Plan	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.
3.5	Cyber Crisis Management Plan	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
3.5	Cyber Crisis Management Plan	<a href="#">ec2-instance-managed-by-systems-manager (p. 132)</a>	An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.
3.5	Cyber Crisis Management Plan	<a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a>	Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment.
3.5	Cyber Crisis Management Plan	<a href="#">ec2-managedinstance-patch-compliance-status-check (p. 136)</a>	Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures.

Control ID	Control Description	AWS Config Rule	Guidance
4.4(g)	Fraud analysis- Suspicious transaction analysis, embezzlement, theft or suspected money-laundering, misappropriation of assets, manipulation of financial records etc. The regulatory requirement of reporting fraud to RBI should be system driven.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
4.4(h)	Capacity and performance analysis of IT security systems.	<a href="#">dynamodb-autoscaling-enabled (p. 128)</a>	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.
4.4(h)	Capacity and performance analysis of IT security systems.	<a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a>	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.

Control ID	Control Description	AWS Config Rule	Guidance
4.4(h)	Capacity and performance analysis of IT security systems.	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
4.4(h)	Capacity and performance analysis of IT security systems.	<a href="#">rds-instance-deletion-protection-enabled (p. 166)</a>	Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.

Control ID	Control Description	AWS Config Rule	Guidance
4.4(h)	Capacity and performance analysis of IT security systems.	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
4.4(h)	Capacity and performance analysis of IT security systems.	<a href="#">s3-bucket-default-lock-enabled (p. 177)</a>	Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data.

Control ID	Control Description	AWS Config Rule	Guidance
4.4(h)	Capacity and performance analysis of IT security systems.	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.
4.4(h)	Capacity and performance analysis of IT security systems.	<a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a>	The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.

Control ID	Control Description	AWS Config Rule	Guidance
4.4(h)	Capacity and performance analysis of IT security systems.	<a href="#">dynamodb-throughput-limit-check (p. 130)</a>	Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set <code>accountRCUThresholdPercentage</code> (Config Default: 80) and <code>accountWCUThresholdPercentage</code> (Config Default: 80) parameters. The actual values should reflect your organization's policies.
4.4(h)	Capacity and performance analysis of IT security systems.	<a href="#">ec2-instance-detailed-monitoring-enabled (p. 132)</a>	Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance.
4.4(h)	Capacity and performance analysis of IT security systems.	<a href="#">lambda-concurrency-check (p. 161)</a>	This rule ensures that a Lambda function's concurrency high and low limits are established. This can assist in baselining the number of requests that your function is serving at any given time.

Control ID	Control Description	AWS Config Rule	Guidance
4.4(h)	Capacity and performance analysis of IT security systems.	<a href="#">lambda-dlq-check (p. 161)</a>	Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed.
4.4(h)	Capacity and performance analysis of IT security systems.	<a href="#">rds-enhanced-monitoring-enabled (p. 165)</a>	Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics.

Control ID	Control Description	AWS Config Rule	Guidance
4.4(h)	Capacity and performance analysis of IT security systems.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.
4.4(h)	Capacity and performance analysis of IT security systems.	<a href="#">ebs-optimized-instance (p. 131)</a>	An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance.
4.4(h)	Capacity and performance analysis of IT security systems.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.

Control ID	Control Description	AWS Config Rule	Guidance
4.4(i)	Incident reporting, their impact and steps taken for non-recurrence of such events in the future.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
4.4(i)	Incident reporting, their impact and steps taken for non-recurrence of such events in the future.	<a href="#">guardduty-non-archived-findings (p. 152)</a>	Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the <code>daysLowSev</code> (Config Default: 30), <code>daysMediumSev</code> (Config Default: 7), and <code>daysHighSev</code> (Config Default: 1) for non-archived findings, as required by your organization's policies.
6.3	NBFCs shall consider the need to put in place necessary backup sites for their critical business systems and Data centers.	<a href="#">dynamodb-autoscaling-enabled (p. 128)</a>	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.

Control ID	Control Description	AWS Config Rule	Guidance
6.3	NBFCs shall consider the need to put in place necessary backup sites for their critical business systems and Data centers.	<a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a>	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.
6.3	NBFCs shall consider the need to put in place necessary backup sites for their critical business systems and Data centers.	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.

Control ID	Control Description	AWS Config Rule	Guidance
6.3	NBFCs shall consider the need to put in place necessary backup sites for their critical business systems and Data centers.	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.
6.3	NBFCs shall consider the need to put in place necessary backup sites for their critical business systems and Data centers.	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.
8.1	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">s3-bucket-policy-grantee-check (p. 178)</a>	Manage access to the AWS Cloud by enabling <code>s3_bucket_policy_grantee_check</code> . This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide.

Control ID	Control Description	AWS Config Rule	Guidance
8.1	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">dms-replication-not-public (p. 127)</a>	Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts.
8.1	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">ebs-snapshot-public-restorable-check (p. 131)</a>	Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts.
8.1	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">ec2-instance-no-public-ip (p. 133)</a>	Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts.
8.1	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">elasticsearch-in-vpc-only (p. 141)</a>	Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection.

Control ID	Control Description	AWS Config Rule	Guidance
8.I	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">emr-master-no-public-ip (p. 146)</a>	Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts.
8.I	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">restricted-ssh (p. 159)</a>	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access.

Control ID	Control Description	AWS Config Rule	Guidance
8.I	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">ec2-instances-in-vpc (p. 159)</a>	Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access.
8.I	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">internet-gateway-authorized-vpc-only (p. 160)</a>	Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources.
8.I	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">lambda-function-public-access-prohibited (p. 161)</a>	Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources.

Control ID	Control Description	AWS Config Rule	Guidance
8.I	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">lambda-inside-vpc (p. 162)</a>	Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC.
8.I	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">rds-instance-public-access-check (p. 166)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts.
8.I	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">rds-snapshots-public-prohibited (p. 168)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.

Control ID	Control Description	AWS Config Rule	Guidance
8.1	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">redshift-cluster-public-access-check (p. 171)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts.
8.1	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">restricted-common-ports (p. 174)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
8.I	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">s3-account-level-public-access-blocks (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies.
8.I	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">s3-bucket-public-read-prohibited (p. 179)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.
8.I	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">s3-bucket-public-write-prohibited (p. 180)</a>	Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data.

Control ID	Control Description	AWS Config Rule	Guidance
8.I	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">sagemaker-notebook-no-direct-internet-access (p. 183)</a>	Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users.
8.I	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">vpc-default-security-group-closed (p. 188)</a>	Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources.
8.I	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">vpc-sg-open-only-to-authorized-ports (p. 189)</a>	Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems.

Control ID	Control Description	AWS Config Rule	Guidance
8.III	A Maker-checker concept to reduce the risk of error and misuse and to ensure reliability of data/information.	<a href="#">s3-bucket-versioning-enabled (p. 181)</a>	Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures.
8.IX	Arrangement for backup of data with periodic testing.	<a href="#">db-instance-backup-enabled (p. 126)</a>	The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements.
8.IX	Arrangement for backup of data with periodic testing.	<a href="#">dynamodb-in-backup-plan (p. 128)</a>	To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	Control Description	AWS Config Rule	Guidance
8.IX	Arrangement for backup of data with periodic testing.	<a href="#">dynamodb-pitr-enabled (p. 129)</a>	Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days.
8.IX	Arrangement for backup of data with periodic testing.	<a href="#">ebs-in-backup-plan (p. 130)</a>	To help with data backup processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
8.IX	Arrangement for backup of data with periodic testing.	<a href="#">efs-in-backup-plan (p. 139)</a>	To help with data backup processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Control ID	Control Description	AWS Config Rule	Guidance
8.IX	Arrangement for backup of data with periodic testing.	<a href="#">elasticache-redis-cluster-automatic-backup-check (p. 140)</a>	When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup.
8.IX	Arrangement for backup of data with periodic testing.	<a href="#">rds-in-backup-plan (p. 167)</a>	To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.
8.IX	Arrangement for backup of data with periodic testing.	<a href="#">s3-bucket-replication-enabled (p. 180)</a>	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained.

Control ID	Control Description	AWS Config Rule	Guidance
8.1	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">access-keys-rotated (p. 107)</a>	The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
8.1	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">emr-kerberos-enabled (p. 145)</a>	The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal.
8.1	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	Control Description	AWS Config Rule	Guidance
8.I	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.

Control ID	Control Description	AWS Config Rule	Guidance
8.I	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
8.1	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
8.1	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">iam-root-access-key-check (p. 157)</a>	Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality.
8.1	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.

Control ID	Control Description	AWS Config Rule	Guidance
8.I	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">iam-user-mfa-enabled (p. 158)</a>	Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users.
8.I	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.
8.I	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
8.I	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">mfa-enabled-for-iam-console-access (p. 163)</a>	Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users.
8.I	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">root-account-hardware-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.
8.I	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">root-account-mfa-enabled (p. 175)</a>	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.

Control ID	Control Description	AWS Config Rule	Guidance
8.I	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">secretsmanager-rotation-enabled-check (p. 183)</a>	This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised.
8.I	Basic security aspects such as physical/ logical access controls and well defined password policy.	<a href="#">secretsmanager-scheduled-rotation-success-check (p. 184)</a>	This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised.
8.II	A well-defined user role.	<a href="#">iam-group-has-users-check (p. 153)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege.

Control ID	Control Description	AWS Config Rule	Guidance
8.II	A well-defined user role.	<a href="#">iam-no-inline-policy-check (p. 154)</a>	Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management.

Control ID	Control Description	AWS Config Rule	Guidance
8.II	A well-defined user role.	<a href="#">iam-password-policy (p. 154)</a>	<p>The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set <code>RequireUppercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireLowercaseCharacters</code> (AWS Foundational Security Best Practices value: true), <code>RequireSymbols</code> (AWS Foundational Security Best Practices value: true), <code>RequireNumbers</code> (AWS Foundational Security Best Practices value: true), <code>MinimumPasswordLength</code> (AWS Foundational Security Best Practices value: 14), <code>PasswordReusePrevention</code> (AWS Foundational Security Best Practices value: 24), and <code>MaxPasswordAge</code> (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies.</p>

Control ID	Control Description	AWS Config Rule	Guidance
8.II	A well-defined user role.	<a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a>	AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
8.II	A well-defined user role.	<a href="#">iam-user-group-membership-check (p. 157)</a>	AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties.
8.II	A well-defined user role.	<a href="#">iam-user-no-policies-check (p. 158)</a>	This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges.

Control ID	Control Description	AWS Config Rule	Guidance
8.II	A well-defined user role.	<a href="#">iam-user-unused-credentials-check (p. 159)</a>	AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the <code>maxCredentialUsageAge</code> (Config Default: 90). The actual value should reflect your organization's policies.
8.1	IT Systems should be progressively scaled up as the size and complexity of NBFC's operations increases.	<a href="#">dynamodb-autoscaling-enabled (p. 128)</a>	Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling.

Control ID	Control Description	AWS Config Rule	Guidance
8.1	IT Systems should be progressively scaled up as the size and complexity of NBFC's operations increases.	<a href="#">elb-cross-zone-load-balancing-enabled (p. 143)</a>	Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances.
8.1	IT Systems should be progressively scaled up as the size and complexity of NBFC's operations increases.	<a href="#">elb-deletion-protection-enabled (p. 144)</a>	This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.
8.1	IT Systems should be progressively scaled up as the size and complexity of NBFC's operations increases.	<a href="#">rds-instance-deletion-protection-enabled (p. 166)</a>	Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications.

Control ID	Control Description	AWS Config Rule	Guidance
8.1	IT Systems should be progressively scaled up as the size and complexity of NBFC's operations increases.	<a href="#">rds-multi-az-support (p. 168)</a>	Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete.
8.1	IT Systems should be progressively scaled up as the size and complexity of NBFC's operations increases.	<a href="#">vpc-vpn-2-tunnels-up (p. 189)</a>	Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway.

Control ID	Control Description	AWS Config Rule	Guidance
8.1	IT Systems should be progressively scaled up as the size and complexity of NBFC's operations increases.	<a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a>	The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance.
8.1	IT Systems should be progressively scaled up as the size and complexity of NBFC's operations increases.	<a href="#">dynamodb-throughput-limit-check (p. 130)</a>	Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set <code>accountRCUThresholdPercentage</code> (Config Default: 80) and <code>accountWCUThresholdPercentage</code> (Config Default: 80) parameters. The actual values should reflect your organization's policies.

Control ID	Control Description	AWS Config Rule	Guidance
8.1	IT Systems should be progressively scaled up as the size and complexity of NBFC's operations increases.	<a href="#">ec2-instance-detailed-monitoring-enabled (p. 132)</a>	Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance.
8.1	IT Systems should be progressively scaled up as the size and complexity of NBFC's operations increases.	<a href="#">guardduty-enabled-centralized (p. 152)</a>	Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment.
8.1	IT Systems should be progressively scaled up as the size and complexity of NBFC's operations increases.	<a href="#">lambda-concurrency-check (p. 161)</a>	This rule ensures that a Lambda function's concurrency high and low limits are established. This can assist in baselining the number of requests that your function is serving at any given time.

Control ID	Control Description	AWS Config Rule	Guidance
8.1	IT Systems should be progressively scaled up as the size and complexity of NBFC's operations increases.	<a href="#">rds-enhanced-monitoring-enabled (p. 165)</a>	Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics.
8.1	IT Systems should be progressively scaled up as the size and complexity of NBFC's operations increases.	<a href="#">securityhub-enabled (p. 186)</a>	AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions.

## Template

The template is available on GitHub: [Operational Best Practices for RBI MD-ITF](#).

## Operational Best Practices for Security, Identity, and Compliance Services

This pack contains AWS Config rules based on Security, Identity, and Compliance Services. For more information, see [Security, Identity, and Compliance on AWS](#). This Conformance Pack has been designed for compatibility with the majority of AWS regions and to not require setting of any Parameters. Additional managed rules that require parameters to be set for your environment and/or for your specific region can be found at: [List of AWS Config Managed Rules](#).

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

See Parameters section for names and descriptions of required parameters.

The template is available on GitHub: [Operational Best Practices for Security, Identity, and Compliance Services](#).

## Operational Best Practices for Serverless

This pack contains AWS Config rules based on Serverless solutions. This Conformance Pack has been designed for compatibility with the majority of AWS regions and to not require setting of any Parameters. Additional managed rules that require parameters to be set for your environment and/or for your specific region can be found at: [List of AWS Config Managed Rules](#).

See Parameters section for names and descriptions of required parameters.

The template is available on GitHub: [Operational Best Practices for Serverless](#).

## Operational Best Practices for Storage Services

This pack contains AWS Config rules based on Storage Services. For more information, see [Cloud Storage on AWS](#). This Conformance Pack has been designed for compatibility with the majority of AWS regions and to not require setting of any Parameters. Additional managed rules that require parameters to be set for your environment and/or for your specific region can be found at: [List of AWS Config Managed Rules](#).

**AWS Region:** All supported AWS Regions except Middle East (Bahrain)

See Parameters section for names and descriptions of required parameters.

The template is available on GitHub: [Operational Best Practices for Storage Services](#).

## Example Templates with Remediation Action

### Operational Best Practices For Amazon DynamoDB with Remediation

The template is available on GitHub: [Operational Best Practices For Amazon DynamoDB with Remediation](#).

### Operational Best Practices For Amazon S3 with Remediation

The template is available on GitHub: [Operational Best Practices For Amazon S3 with Remediation](#).

## Custom Conformance Pack

The template is available on GitHub: [Custom Conformance Pack](#).

For more information about template structure, see [Template Anatomy](#) in the AWS CloudFormation User Guide.

## Viewing Compliance Data in the Conformance Packs Dashboard

The main page for **Conformance Packs** displays all of the conformance packs that you currently have in your AWS account. The page also contains the name, deployment status, and compliance status of each conformance pack.

### Navigating the Conformance Packs Main Page

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.
  2. Navigate to the **Conformance packs** page. Review your conformance packs and their compliance states. You can then do the following:
    - To add and configure a new conformance pack, choose **Deploy conformance pack**.
    - To delete a conformance pack and its data, change the configuration settings, or view additional details, such as the delivery location or parameters, choose a conformance pack and choose **Actions**.
- Note**  
You cannot edit a deployed conformance pack. You can modify the other selections at any time by choosing the name of the conformance pack and **Edit** in the **Actions** dropdown.
- To view the history of compliance state changes and adjust remediation actions to meet compliance goals, choose a conformance pack and choose **Conformance pack timeline**.

### Learn more

[Conformance Pack Prerequisites](#)

[Conformance Pack Sample Templates](#)

[Deploying a Conformance Pack](#)

[AWS Service Limits](#)

## Deploying a Conformance Pack Using the AWS Config Console

On the **Conformance packs** page, you can deploy a conformance pack for an account in a Region. You can also edit and delete the deployed conformance pack.

## Deploy a Conformance Pack Using Sample Templates

You can deploy a conformance pack using AWS Config sample templates.

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. Navigate to the **Conformance packs** page and choose **Deploy conformance pack**.
3. On the **Specify template** page, either choose a sample template or use an existing template.
  - If you choose **Use sample template**, select a **Sample template** from the drop-down list of sample templates.

For information about the contents of each template, see Conformance Pack Sample Templates.

- If you choose **Template is ready**, specify the template source. It is either an Amazon S3 URI or a template that you upload.

If your template is more than 50 KB, upload it to the S3 bucket and select that S3 bucket location.  
For example: `s3://bucketname/prefix`.

4. Choose **Next**.
5. On the **Specify conformance pack details** page, type the name for your conformance pack.

The conformance pack name must be a unique name with a maximum of 256 alphanumeric characters. The name can contain hyphens but cannot contain spaces.

6. Optional: Add a parameter.

Parameters are defined in your template and help you manage and organize your resources.

7. Choose **Next**.
8. On the **Review and deploy** page, review all of the information.

You can edit the template details and conformance pack details by choosing **Edit**.

9. Choose **Deploy conformance pack**.

AWS Config displays the conformance pack on the conformance pack page with the appropriate status.

If your conformance pack deployment fails, check your permissions, verify that you did the prerequisite steps, and try again. Or you can contact AWS Config support.

To deploy a **conformance pack using sample template with remediations**, see the [Prerequisites for Using a Conformance Pack With Remediation \(p. 219\)](#) and then use the preceding procedure.

To deploy a **conformance pack with one or more AWS Config rules**, see the [Prerequisites for Using a Conformance Pack With One or More AWS Config Rules \(p. 220\)](#).

## Edit a Conformance Pack

1. To edit a conformance pack, select the conformance pack from the table.
2. Choose **Actions** and then choose **Edit**.
3. On the **Edit conformance pack** page, you can edit the template details, sample template, conformance pack, and parameters section.

You cannot change the name of the conformance pack.

4. Choose **Save changes**.

The conformance pack is displayed with the AWS Config rules.

## Delete a Conformance Pack

1. To delete a conformance pack, select the conformance pack from the table.
2. Choose **Actions** and then choose **Delete**.
3. On the delete *conformance pack* dialog box, confirm if you would like to permanently delete this conformance pack.

You cannot revert this action. When you delete a conformance pack, you delete all of the AWS Config rules and remediation actions in that conformance pack.

4. Enter **Delete** and choose **Delete**.

On the **Conformance packs** page, you can see the deployment status as **Deleting** until the conformance pack is completely deleted.

## Deploying a Conformance Pack Using the AWS Command Line Interface

You can deploy, view, update, view compliance status, and delete an AWS Config conformance pack using the AWS Command Line Interface (AWS CLI).

To install the AWS CLI on your local machine see, [AWS Config Conforms Amazon S3 bucket](#).

If necessary, type `aws configure` to configure the AWS CLI to use an AWS Region where AWS Config conformance packs are available.

### Topics

- [Deploy a Conformance Pack \(p. 3254\)](#)
- [View a Conformance Pack \(p. 3255\)](#)
- [View Conformance Pack Status \(p. 3255\)](#)
- [View Conformance Pack Compliance Status \(p. 3256\)](#)
- [Get Compliance Details for a Specific Conformance Pack \(p. 3256\)](#)
- [Delete a Conformance Pack \(p. 3257\)](#)

## Deploy a Conformance Pack

1. Open a command prompt or a terminal window.
2. Type the following command to deploy a conformance pack named **MyConformancePack1**.

```
aws configservice put-conformance-pack --conformance-pack-name="MyConformancePack1"
--template-s3-uri="s3://AmazonS3bucketname/template name.yaml" --delivery-s3-
bucket=AmazonS3bucketname
```

OR

You can also upload a YAML template from your local directory.

```
aws configservice put-conformance-pack --conformance-pack-name="MyConformancePack1" --  
template-body=template body --delivery-s3-bucket=AmazonS3bucketname
```

3. Press Enter to run the command.

You should see output similar to the following.

```
{  
  "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-pack/  
MyConformancePack1/conformance-pack-ID"  
}
```

## View a Conformance Pack

1. Type the following command.

```
aws configservice describe-conformance-packs
```

OR

```
aws configservice describe-conformance-packs --conformance-pack-  
name="MyConformancePack1"
```

2. You should see output similar to the following.

```
{  
  "conformancePackName": "MyConformancePack1",  
  "conformancePackId": "conformance-pack-ID",  
  "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-pack/  
MyConformancePack1/conformance-pack-ID",  
  "conformancePackInputParameters": [],  
  "lastUpdateRequestedTime": "Thu Jul 18 16:07:05 PDT 2019"  
}
```

## View Conformance Pack Status

1. Type the following command.

```
aws configservice describe-conformance-pack-status --conformance-pack-  
name="MyConformancePack1"
```

2. You should see output similar to the following .

```
{  
  "stackArn": "arn:aws:cloudformation:us-west-2:AccountID:stack/awsconfigconforms-  
MyConformancePack1-conformance-pack-ID/d4301fe0-a9b1-11e9-994d-025f28dd83ba",  
  "conformancePackName": "MyConformancePack1",  
  "conformancePackId": "conformance-pack-ID",  
  "lastUpdateCompletedTime": "Thu Jul 18 16:15:17 PDT 2019",  
  "conformancePackState": "CREATE_COMPLETE",  
  "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-pack/  
MyConformancePack1/conformance-pack-ID",  
  "lastUpdateRequestedTime": "Thu Jul 18 16:14:35 PDT 2019"
```

```
}
```

## View Conformance Pack Compliance Status

1. Type the following command.

```
aws configservice describe-conformance-pack-compliance --conformance-pack-name="MyConformancePack1"
```

2. You should see output similar to the following.

```
{
  "conformancePackName": "MyConformancePack1",
  "conformancePackRuleComplianceList": [
    {
      "configRuleName": "awsconfigconforms-RuleName1-conformance-pack-ID",
      "complianceType": "NON_COMPLIANT"
    },
    {
      "configRuleName": "awsconfigconforms-RuleName2-conformance-pack-ID",
      "complianceType": "COMPLIANT"
    }
  ]
}
```

## Get Compliance Details for a Specific Conformance Pack

1. Type the following command.

```
aws configservice get-conformance-pack-compliance-details --conformance-pack-name="MyConformancePack1"
```

2. You should see output similar to the following.

```
{
  "conformancePackRuleEvaluationResults": [
    {
      "evaluationResultIdentifier": {
        "orderingTimestamp": "Tue Jul 16 23:07:35 PDT 2019",
        "evaluationResultQualifier": {
          "resourceId": "resourceID",
          "configRuleName": "awsconfigconforms-RuleName1-conformance-pack-ID",
          "resourceType": "AWS:::Account"
        }
      },
      "configRuleInvokedTime": "Tue Jul 16 23:07:50 PDT 2019",
      "resultRecordedTime": "Tue Jul 16 23:07:51 PDT 2019",
      "complianceType": "NON_COMPLIANT"
    },
    {
      "evaluationResultIdentifier": {
        "orderingTimestamp": "Thu Jun 27 15:16:36 PDT 2019",
        "evaluationResultQualifier": {
          "resourceId": "resourceID",
```

```
        "configRuleName": "awsconfigconforms-RuleName2-conformance-pack-ID",
        "resourceType": "AWS::EC2::SecurityGroup"
    },
    "configRuleInvokedTime": "Thu Jul 11 23:08:06 PDT 2019",
    "resultRecordedTime": "Thu Jul 11 23:08:06 PDT 2019",
    "complianceType": "COMPLIANT"
},
"conformancePackName": "MyConformancePack1"
}
```

## Delete a Conformance Pack

- Type the following command.

```
aws configservice delete-conformance-pack --conformance-pack-name MyConformancePack1
```

If successful, the command runs with no additional output.

## Managing Conformance Packs (API)

Use the following AWS Config API actions to manage conformance packs:

- [DeleteConformancePack](#)
- [DescribeConformancePackCompliance](#)
- [DescribeConformancePacks](#)
- [DescribeConformancePackStatus](#)
- [GetConformancePackComplianceDetails](#)
- [GetConformancePackComplianceSummary](#)
- [PutConformancePack](#)

## Managing Conformance Packs Across all Accounts in Your Organization

Use AWS Config to manage conformance packs across all AWS accounts within an organization. You can do the following:

- Centrally deploy, update, and delete conformance packs across member accounts in an organization in AWS Organizations.
- Deploy a common set of AWS Config rules and remediation actions across all accounts and specify accounts where AWS Config rules and remediation actions should not be created.
- Use the APIs from the master account in AWS Organizations to enforce governance by ensuring that the underlying AWS Config rules and remediation actions are not modifiable by your organization's member accounts.

### Note

*For deployments across different regions*

The API call to deploy rules and conformance packs across accounts is region specific. At the organization level, you need to change the context of your API call to a different region if you want to deploy rules in other regions. For example, to deploy a rule in US East (N. Virginia), change the region to US East (N. Virginia) and then call `PutOrganizationConfigRule`.

*For accounts within an organization*

If a new account joins an organization, the rule is deployed to that account. When an account leaves an organization, the rule is removed.

Ensure AWS Config recording is on before you use the following APIs to manage conformance pack rules across all AWS accounts within an organization:

- [DeleteOrganizationConformancePack](#), deletes the specified organization conformance pack and all of the config rules and remediation actions from all member accounts in that organization.
- [DescribeOrganizationConformancePacks](#), returns a list of organization conformance packs.
- [DescribeOrganizationConformancePackStatuses](#), provides organization conformance pack deployment status for an organization.
- [GetOrganizationConformancePackDetailedStatus](#), returns detailed status for each member account within an organization for a given organization conformance pack.
- [PutOrganizationConformancePack](#), deploys conformance packs across member accounts in an AWS Organization.

## Viewing Compliance History Timeline for Conformance Packs

AWS Config supports storing compliance state changes to your conformance packs. This allows you to view the history of compliance state changes and adjust remediation actions to meet compliance goals. These compliance state changes are presented as a timeline. The timeline captures changes as `ConfigurationItems` over a period of time. You can also use this feature to find specific rules within a conformance pack that are non-compliant.

You can opt in or out to record all resource types in AWS Config. If you have opted to record all resource types, AWS Config automatically begins recording the conformance pack compliance history as evaluated by AWS Config Rules. By default, AWS Config records the configuration changes for all supported resources. You can also select only the specific conformance pack compliance history resource type: `AWS::Config::ConformancePackCompliance`. Recording for the `AWS::Config::ConformancePackCompliance` resource type is available at no additional charge. For more information, see [Selecting Which Resources AWS Config Records](#).

A conformance pack is compliant if all of the rules in a conformance packs are compliant. It is noncompliant if any of the rules are not compliant. The compliance status of a conformance pack is `INSUFFICIENT_DATA` only if all rules within a conformance pack cannot be evaluated due to insufficient data. If some of the rules in a conformance pack are compliant but the compliance status of other rules in that same conformance pack is `INSUFFICIENT_DATA`, the conformance pack shows compliant. Compliance for a conformance pack is not evaluated all at once. Some rules may take a longer time to evaluate than others. Compliance is evaluated for groups of rules at a time, continuing in stages until all the rules in a conformance pack have been evaluated.

### Topics

- [Viewing the Compliance Timeline \(p. 3259\)](#)
- [Querying Compliance History \(p. 3259\)](#)

## Viewing the Compliance Timeline

Access the compliance timeline by selecting a specific conformance pack from the **Conformance pack** main page.

1. Navigate to the **Conformance Pack** page.
2. On the **Conformance Pack** main page, choose a specific conformance pack and then choose **Conformance pack timeline**.

### Note

Alternatively, you can use the compliance timeline from the conformance pack's details page. Choose a conformance pack and choose **View details** in the **Actions** dropdown. From this page, choose **Conformance pack timeline**.

The timeline shows you the history of compliance state changes for a conformance pack. You can do the following:

1. Adjust remediation actions to meet compliance goals.
2. Expand a compliance change to view the line-by-line compliance status of each rule within a conformance pack.
3. From the expanded view, choose a specific rule to view its details page.

## Querying Compliance History

Query the compliance history using `get-resource-config-history` using the resource type `AWS::Config::ConformancePackCompliance`.

```
aws configservice get-resource-config-history --resource-type  
AWS::Config::ConformancePackCompliance --resource-id conformance-pack-ID
```

You should see output similar to the following:

```
{  
  "configurationItems": [  
    {  
      "version": "1.3",  
      "accountId": "Account ID",  
      "configurationItemCaptureTime": 1614641951.442,  
      "configurationItemStatus": "OK",  
      "configurationStateId": "1614641951442",  
      "configurationItemMD5Hash": "",  
      "arn": "arn:aws:config:us-east-1:Account ID:conformance-  
pack/MyConformancePack1/conformance-pack-ID",  
      "resourceType": "AWS::Config::ConformancePackCompliance",  
      "resourceId": "conformance-pack-ID",  
      "resourceName": "MyConformancePack1",  
      "awsRegion": "us-east-1",  
      "tags": {},  
      "relatedEvents": [],  
      "relationships": [],  
      "configuration": "{\n\"compliantRuleCount\":1,\n\"configRuleList\":  
[{\n\"configRuleName\":\n\"RuleName1-conformance-pack-ID\",\n\"controls\":[],\n\"configRuleArn\n\":\n\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-  
conforms.amazonaws.com/config-rule-nnnnnn\",\n\"complianceType\":\n\"INSUFFICIENT_DATA\"},  
{\n\"configRuleName\":\n\"RuleName2-conformance-pack-ID\",\n\"controls\":[],\n\"configRuleArn\n\":\n\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-  
conforms.amazonaws.com/config-rule-mmmmmm\",\n\"complianceType\":\n\"COMPLIANT\"},
```

```
{
  "configRuleName": "RuleName3-conformance-pack-ID",
  "controls": [],
  "configRuleArn": "arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-conforms.amazonaws.com/config-rule-pppppp",
  "complianceType": "INSUFFICIENT_DATA",
  "totalRuleCount": 3,
  "nonCompliantRuleCount": 0,
  "complianceType": "COMPLIANT",
  "supplementaryConfiguration": {}
},
{
  "version": "1.3",
  "accountId": "768311917693",
  "configurationItemCaptureTime": 1605551029.515,
  "configurationItemStatus": "ResourceDiscovered",
  "configurationStateId": "1605551029515",
  "configurationItemMD5Hash": "",
  "resourceType": "AWS::Config::ConformancePackCompliance",
  "resourceId": "conformance-pack-ID",
  "resourceName": "MyConformancePack1",
  "awsRegion": "us-east-1",
  "tags": {},
  "relatedEvents": [],
  "relationships": [],
  "configuration": "{
    \"compliantRuleCount\": 1,
    \"configRuleList\": [
      {
        \"configRuleName\": \"RuleName1-conformance-pack-ID\",
        \"controls\": [],
        \"configRuleArn\": \"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-conforms.amazonaws.com/config-rule-nnnnnn\",
        \"complianceType\": \"INSUFFICIENT_DATA\"
      },
      {
        \"configRuleName\": \"RuleName2-conformance-pack-ID\",
        \"controls\": [],
        \"configRuleArn\": \"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-conforms.amazonaws.com/config-rule-mmmmmm\",
        \"complianceType\": \"COMPLIANT\"
      },
      {
        \"configRuleName\": \"RuleName3-conformance-pack-ID\",
        \"controls\": [],
        \"configRuleArn\": \"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-conforms.amazonaws.com/config-rule-pppppp\",
        \"complianceType\": \"INSUFFICIENT_DATA\"
      }
    ],
    \"totalRuleCount\": 3,
    \"nonCompliantRuleCount\": 0,
    \"complianceType\": \"COMPLIANT\"
  }"
}
]
```

For more information, see [Supported Resource Types \(AWS Config\)](#) and [GetResourceConfigHistory](#) in the API reference.

## Troubleshooting

If you get an error indicating that the conformance pack failed while creating, updating, or deleting it, you can check the status of your conformance pack.

```
aws configservice describe-conformance-pack-status --conformance-pack-name=ConformancePackName
```

You should see output similar to the following.

```
"ConformancePackStatusDetails": [
  {
    "ConformancePackName": "ConformancePackName",
    "ConformancePackId": "ConformancePackId",
    "ConformancePackArn": "ConformancePackArn",
    "ConformancePackState": "CREATE_FAILED",
    "StackArn": "CloudFormation stackArn",
    "ConformancePackStatusReason": "Failure Reason",
    "LastUpdateRequestedTime": 1573865201.619,
    "LastUpdateCompletedTime": 1573864244.653
  }
]
```

]

Check the **ConformancePackStatusReason** for information about the failure.

#### **When the stackArn is present in the response**

If the error message is not clear or if the failure is due to an internal error, go to the AWS CloudFormation console and do the following:

1. Search for the **stackArn** from the output.
2. Choose the **Events** tab of the AWS CloudFormation stack and check for failed events.

The status reason indicates why the conformance pack failed.

#### **When the stackArn is not present in the response**

If you receive a failure while you create a conformance pack but the **stackArn** is not present in the status response, the possible reason is that the stack creation failed and AWS CloudFormation rolled back and deleted the stack. Go to the AWS CloudFormation console and search for stacks that are in a **Deleted** state. The failed stack might be available there. The AWS CloudFormation stack contains the conformance pack name. If you find the failed stack, choose the **Events** tab of the AWS CloudFormation stack and check for failed events.

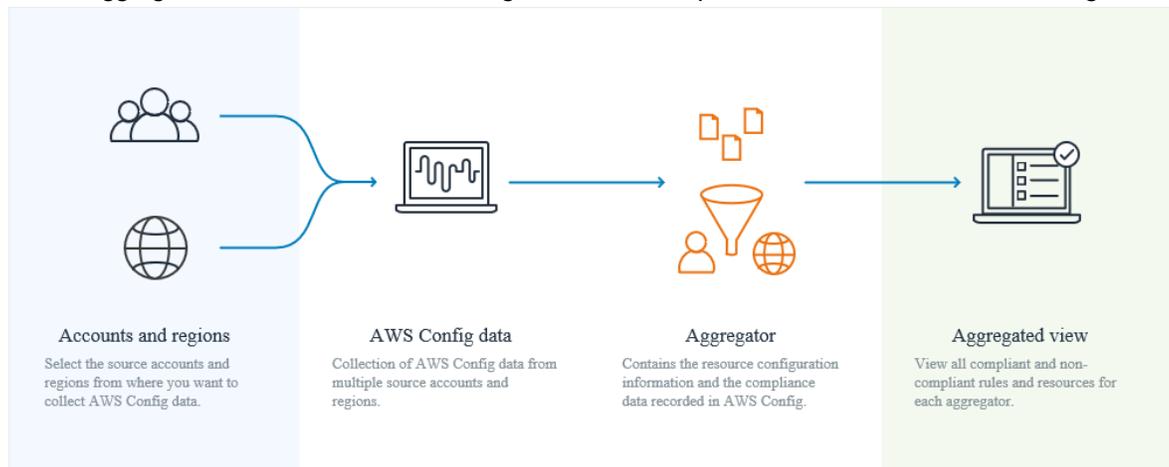
If none of these steps worked and if the failure reason is an internal service error, then try operation again or contact AWS Config support.

# Multi-Account Multi-Region Data Aggregation

An aggregator is an AWS Config resource type that collects AWS Config configuration and compliance data from the following:

- Multiple accounts and multiple regions.
- Single account and multiple regions.
- An organization in AWS Organizations and all the accounts in that organization which have AWS Config enabled.

Use an aggregator to view the resource configuration and compliance data recorded in AWS Config.



For more information about concepts, see [Multi-Account Multi-Region Data Aggregation \(p. 5\)](#) section in the Concepts topic.

To collect your AWS Config data from source accounts and regions, start with:

1. Adding an aggregator to aggregate AWS Config configuration and compliance data from multiple accounts and regions.
2. Authorizing aggregator accounts to collect AWS Config configuration and compliance data. Authorization is required when your source accounts are individual accounts. Authorization is not required if you are aggregating source accounts that are part of AWS Organizations.
3. Monitoring compliance data for rules and accounts in the aggregated view.

## Region Support

Currently, multi-account multi-region data aggregation is supported in the following regions:

Region Name	Region	Endpoint	Protocol
Africa (Cape Town)	af-south-1	config.af-south-1.amazonaws.com	HTTPS

Region Name	Region	Endpoint	Protocol
Middle East (Bahrain)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Asia Pacific (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asia Pacific (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia Pacific (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asia Pacific (Singapore)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pacific (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
AWS GovCloud (US-East)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (US-West)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS
Canada (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Europe (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europe (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europe (Ireland)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europe (London)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europe (Milan)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europe (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
South America (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS

Region Name	Region	Endpoint	Protocol
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
US West (N. California)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS

## Learn More

- [Concepts \(p. 2\)](#)
- [Viewing Compliance Data in the Aggregator Dashboard \(p. 3264\)](#)
- [Setting Up an Aggregator Using the Console \(p. 3266\)](#)
- [Setting Up an Aggregator Using the AWS Command Line Interface \(p. 3268\)](#)
- [Authorizing Aggregator Accounts to Collect AWS Config Configuration and Compliance Data Using the Console \(p. 3274\)](#)
- [Authorizing Aggregator Accounts to Collect AWS Config Configuration and Compliance Data Using the AWS Command Line Interface \(p. 3275\)](#)
- [Troubleshooting for Multi-Account Multi-Region Data Aggregation \(p. 3277\)](#)

## Viewing Compliance Data in the Aggregator Dashboard

The dashboard on the **Aggregators** page displays the configuration data of AWS resources and provides an overview of your rules and conformance packs and their compliance states.

It provides the total resource count of AWS resources. The resource types and source accounts are ranked by the highest number of resources. It also provides a count of compliant and noncompliant rules and conformance packs. The noncompliant rules are ranked by highest number of noncompliant resources. The noncompliant conformance packs and source accounts are ranked by the highest number of noncompliant rules.

After setup, AWS Config starts aggregating data from the specified source accounts into an aggregator. It might take a few minutes for AWS Config to display the compliance status of rules on this page.

### Using the Aggregator Dashboard

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. Navigate to the **Aggregators** page. Review your rules and their compliance states; conformance packs and their compliance states, and AWS resources and their configuration data. You can do the following:
  - Choose an aggregator from the dashboard and filter through your aggregators by AWS region, or account ID.

- View the top ten resource types, in the descending order according to the number of resources. Choose view all resources to go to the **Aggregated resources** page. On this page, you can view all the aggregated resources for an account.
- View the top five accounts by the number of resources, in the descending order according to the number of resources. Choose the number of resources for an account to go to the **Aggregated Resources** page. On this page, you can view all the aggregated resources for an account.
- View the top five noncompliant rules, in descending order according to the number of noncompliant resources. Choose a rule to go to the **Rule details** page.
- View the top five accounts by noncompliant rules, in descending order according to the number of noncompliant rules. Choose an account to go to the **Aggregated Rules** page. On this page, you can view all the aggregated rules for an account.
- View the top five accounts by noncompliant conformance packs, in descending order according to the number of noncompliant conformance packs. Choose an account to go to the **Aggregated Conformance Pack** page. On this page, you can view all the aggregated conformance packs for an account.

#### Note

Data displayed on the tiles is subject to delays.

The **Data collection from all source accounts and regions is incomplete** message is displayed in the aggregated view for the following reasons:

- AWS Config noncompliant rules and configuration data of AWS resources transfer is in progress.
- AWS Config can't find rules to match the filter. Select the appropriate account or region and try again.

The **Data collection from your organization is incomplete. You can view the below data only for 24 hours.** message is displayed in the aggregated view for the following reasons:

- AWS Config is unable to access your organization details due to invalid IAM role. If the IAM role is invalid for more than 24 hours, AWS Config deletes data for entire organization.
- AWS Config service access is disabled in your organization.

3. In the navigation pane, choose **Aggregators** and then choose one of the following options from the dropdown menu to go its aggregated page:

- **Conformance packs**

View all conformance packs that are created and linked to the different AWS accounts within your aggregator. The **Conformance Pack** page displays a table that lists the name, Region, account ID, and compliance status of each conformance pack. From this page, you can choose a conformance pack and **View details** for more information about its rules and resources and their compliance status.

- **Rules**

View all rules that are created and linked to the different AWS accounts within your aggregator. The **Rules** page displays a table that lists the name, compliance status, Region, and account of each rule. From this page, you can choose a rule and **View details** for information, such as its aggregator, Region, account ID, and resources in scope.

- **Resources**

View all resources that are recorded and linked to the different AWS accounts within your aggregator. From the **Resource** page, choose a resource and **View details** to view its details and the rules associated with it and the current resource configuration. You can also see information

about the resource, such as its aggregator, Region, account ID, resource name, resource type, and resource ID.

- **Authorizations**

View all accounts currently authorized or pending authorization. From the **Authorizations** page, choose **Add authorization** to provide access to another account. Choose **Delete authorization** to revoke access from an account ID.

## Learn More

- [Concepts \(p. 2\)](#)
- [Viewing Compliance Data in the Aggregator Dashboard \(p. 3264\)](#)
- [Setting Up an Aggregator Using the Console \(p. 3266\)](#)
- [Authorizing Aggregator Accounts to Collect AWS Config Configuration and Compliance Data Using the Console \(p. 3274\)](#)
- [Troubleshooting for Multi-Account Multi-Region Data Aggregation \(p. 3277\)](#)

# Setting Up an Aggregator Using the Console

On the **Aggregator** page, you can do the following:

- Create an aggregator by specifying the source account IDs or organization and regions from which you want to aggregate data.
- Edit and delete an aggregator.

### Topics

- [Add an Aggregator \(p. 3266\)](#)
- [Edit an Aggregator \(p. 3267\)](#)
- [Delete an Aggregator \(p. 3268\)](#)
- [Learn More \(p. 3266\)](#)

## Add an Aggregator

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. Navigate to the **Aggregators** page and choose **Add aggregator**.
3. **Allow data replication**, gives permission to AWS Config to replicate data from the source accounts into an aggregator account.

Choose **Allow AWS Config to replicate data from source account(s) into an aggregator account**. **You must select this checkbox to continue to add an aggregator.**

4. For **Aggregator name**, type the name for your aggregator.

The aggregator name must be a unique name with a maximum of 64 alphanumeric characters. The name can contain hyphens and underscores.

5. For **Select source accounts**, either choose **Add individual account IDs** or **Add my organization** from which you want to aggregate data.

**Note**

Authorization is required when using **Add individual account IDs** to select source accounts.

- If you choose **Add individual account IDs**, you can add individual account IDs for an aggregator account.
  1. Choose **Add source accounts** to add account IDs.
  2. Choose **Add AWS account IDs** to manually add comma-separated AWS account IDs. If you want to aggregate data from the current account, type the account ID of the account.

OR

Choose **Upload a file** to upload a file (.txt or .csv) of comma-separated AWS account IDs.

3. Choose **Add source accounts** to confirm your selection.
- If you choose **Add my organization**, you can add all accounts in your organization to an aggregator account.

**Note**

Authorization is not required when using **Add my organization** to select source accounts. You must be signed in to the management account or a registered delegated administrator and all the features must be enabled in your organization. If the caller is a management account, AWS Config calls `EnableAwsServiceAccess` API to [enable integration](#) between AWS Config and AWS Organizations. If the caller is a registered delegated administrator, AWS Config calls `ListDelegatedAdministrators` API to verify whether the caller is a valid delegated administrator.

Ensure that the management account registers delegated administrator for AWS Config service principle name (config.amazonaws.com) before the delegated administrator creates an aggregator. To register a delegated administrator, see [Register a Delegated Administrator \(p. 3270\)](#).

1. Choose **Choose IAM role** to create an IAM role or choose an existing IAM role from your account.

You must assign an IAM role to allow AWS Config to call read-only APIs for your organization.

2. Choose **Create a role** and type the IAM role name to create IAM role.

OR

Choose **Choose a role from your account** to select an existing IAM role.

**Note**

In the IAM console, attach the `AWSConfigRoleForOrganizations` managed policy to your IAM role. Attaching this policy allows AWS Config to call AWS Organizations `DescribeOrganization`, `ListAWSServiceAccessForOrganization`, and `ListAccounts` APIs. By default `config.amazonaws.com` is automatically specified as a trusted entity.

3. Choose **Choose IAM role** to confirm your selection.
6. For **Regions**, choose the regions for which you want to aggregate data.
    - Select one region or multiple regions or all the AWS regions.
    - Select **Include future AWS regions** to aggregate data from all future AWS regions where multi-account multi-region data aggregation is enabled.
  7. Choose **Save**. AWS Config displays the aggregator.

## Edit an Aggregator

1. To make changes to the aggregator, choose the aggregator name.

2. Choose **Actions** and then choose **Edit**.
3. Use the sections on the **Edit aggregator** page to change the source accounts, IAM roles, or regions for the aggregator.

**Note**

You cannot change source type from individual account(s) to organization and vice versa.

4. Choose **Save**.

## Delete an Aggregator

1. To delete an aggregator, choose the aggregator name.
2. Choose **Actions** and then choose **Delete**.

A warning message is displayed. Deleting an aggregator results in the loss of all aggregated data. You cannot recover this data but data in the source account(s) is not impacted.

3. Choose **Delete** to confirm your selection.

## Learn More

- [Concepts \(p. 2\)](#)
- [Authorizing Aggregator Accounts to Collect AWS Config Configuration and Compliance Data Using the Console \(p. 3274\)](#)
- [Viewing Compliance Data in the Aggregator Dashboard \(p. 3264\)](#)
- [Troubleshooting for Multi-Account Multi-Region Data Aggregation \(p. 3277\)](#)

# Setting Up an Aggregator Using the AWS Command Line Interface

You can create, view, update, and delete AWS Config aggregator data using the AWS Command Line Interface (AWS CLI). To use the AWS Management Console, see [Setting Up an Aggregator Using the Console \(p. 3266\)](#).

The AWS CLI is a unified tool to manage your AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and use scripts to automate them.

To install the AWS CLI on your local machine, see [Installing the AWS CLI](#) in the *AWS CLI User Guide*.

If necessary, type `aws configure` to configure the AWS CLI to use an AWS Region where AWS Config aggregators are available.

### Topics

- [Add an Aggregator Using Individual Accounts \(p. 3269\)](#)
- [Add an Aggregator Using AWS Organizations \(p. 3270\)](#)
- [Register a Delegated Administrator \(p. 3270\)](#)
- [View an Aggregator \(p. 3271\)](#)
- [Edit an Aggregator \(p. 3272\)](#)

- [Delete an Aggregator \(p. 3273\)](#)
- [Learn More \(p. 3266\)](#)

## Add an Aggregator Using Individual Accounts

1. Open a command prompt or a terminal window.
2. Type the following command to create an aggregator named **MyAggregator**.

```
aws configservice put-configuration-aggregator --configuration-aggregator-name
MyAggregator --account-aggregation-sources "[{\\"AccountIds\\": [\\"AccountID1\\",
\\"AccountID2\\",\\"AccountID3\\"],\\"AllAwsRegions\\": true}]"
```

For `account-aggregation-sources`, type one of the following.

- A comma-separated list of AWS account IDs for which you want to aggregate data. Wrap the account IDs in square brackets, and be sure to escape quotation marks (for example, `[{\\"AccountIds\\": [\\"AccountID1\\",\\"AccountID2\\",\\"AccountID3\\"],\\"AllAwsRegions\\": true}]`).
- You can also upload a JSON file of comma-separated AWS account IDs. Upload the file using the following syntax: `--account-aggregation-sources MyFilePath/MyFile.json`

The JSON file must be in the following format:

```
[
  {
    "AccountIds": [
      "AccountID1",
      "AccountID2",
      "AccountID3"
    ],
    "AllAwsRegions": true
  }
]
```

3. Press Enter to execute the command.

You should see output similar to the following:

```
{
  "ConfigurationAggregator": {
    "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
    "CreationTime": 1517942461.442,
    "ConfigurationAggregatorName": "MyAggregator",
    "AccountAggregationSources": [
      {
        "AllAwsRegions": true,
        "AccountIds": [
          "AccountID1",
          "AccountID2",
          "AccountID3"
        ]
      }
    ],
    "LastUpdatedTime": 1517942461.442
  }
}
```

## Add an Aggregator Using AWS Organizations

Before you begin this procedure, you must be signed in to the management account or a registered delegated administrator and all the features must be enabled in your organization.

### Note

Ensure that the management account registers a delegated administrator for AWS Config service principle name (config.amazonaws.com) before the delegated administrator creates an aggregator. To register a delegated administrator, see [Register a Delegated Administrator \(p. 3270\)](#).

1. Open a command prompt or a terminal window.
2. Type the following command to create an aggregator named **MyAggregator**.

```
aws configservice put-configuration-aggregator --configuration-aggregator-name
MyAggregator --organization-aggregation-source "{\"RoleArn\": \"Complete-Arn\",
\"AllAwsRegions\": true}"
```

3. Press Enter to execute the command.

You should see output similar to the following:

```
{
  "ConfigurationAggregator": {
    "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
    "CreationTime": 1517942461.442,
    "ConfigurationAggregatorName": "MyAggregator",
    "OrganizationAggregationSource": {
      "AllAwsRegions": true,
      "RoleArn": "arn:aws:config:Region:AccountID:config-aggregator/config-
aggregator-floqpus3"
    },
    "LastUpdatedTime": 1517942461.442
  }
}
```

## Register a Delegated Administrator

Delegated administrators are accounts within a given AWS Organization that are granted additional administrative privileges for a specified AWS service.

1. Login with management account credentials.
2. Open a command prompt or a terminal window.
3. Type the following command to enable service access:

```
aws organizations enable-aws-service-access --service-principal config.amazonaws.com
```

4. To verify if the enable service access is complete, type the following command and press Enter to execute the command.

```
aws organizations list-aws-service-access-for-organization
```

You should see output similar to the following:

```
{
```

```
"EnabledServicePrincipals": [  
  {  
    "ServicePrincipal": "config.amazonaws.com",  
    "DateEnabled": 1607020860.881  
  }  
]
```

5. Next, type the following command to register a member account as a delegated administrator for AWS Config.

```
aws organizations register-delegated-administrator --service-principal  
config.amazonaws.com --account-id MemberAccountID
```

6. To verify if the registration of delegated administrator is complete, type the following command and press Enter to execute the command.

```
aws organizations list-delegated-administrators --service-principal  
config.amazonaws.com
```

You should see output similar to the following:

```
{  
  "DelegatedAdministrators": [  
    {  
      "Id": "MemberAccountID",  
      "Arn": "arn:aws:organizations::MemeberAccountID:account/o-  
c7esubdi38/DelegatedAdministratorAccountID",  
      "Email": "name@amazon.com",  
      "Name": "name",  
      "Status": "ACTIVE",  
      "JoinedMethod": "INVITED",  
      "JoinedTimestamp": 1604867734.48,  
      "DelegationEnabledDate": 1607020986.801  
    }  
  ]  
}
```

## View an Aggregator

1. Type the following command:

```
aws configservice describe-configuration-aggregators
```

2. Depending on your source account you should see output similar to the following:

### For individuals accounts

```
{  
  "ConfigurationAggregators": [  
    {  
      "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-  
aggregator/config-aggregator-floppus3",  
      "CreationTime": 1517942461.442,  
      "ConfigurationAggregatorName": "MyAggregator",  
      "AccountAggregationSources": [  
        {  
          "AllAwsRegions": true,  

```

```
        "AccountIds": [
            "AccountID1",
            "AccountID2",
            "AccountID3"
        ]
    },
    "LastUpdatedTime": 1517942461.455
}
]
```

OR

#### For an organization

```
{
  "ConfigurationAggregator": {
    "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
    "CreationTime": 1517942461.442,
    "ConfigurationAggregatorName": "MyAggregator",
    "OrganizationAggregationSource": {
      "AllAwsRegions": true,
      "RoleArn": "arn:aws:config:Region:AccountID:config-aggregator/config-
aggregator-floqpus3"
    },
    "LastUpdatedTime": 1517942461.442
  }
}
```

## Edit an Aggregator

1. You can use the `put-configuration-aggregator` command to update or edit a configuration aggregator.

Type the following command to add a new account ID to **MyAggregator**:

```
aws configservice put-configuration-aggregator --configuration-aggregator-name
MyAggregator --account-aggregation-sources "[{\"AccountIds\": [\"AccountID1\",
\"AccountID2\", \"AccountID3\"], \"AllAwsRegions\": true}]"
```

2. Depending on your source account you should see output similar to the following:

#### For individuals accounts

```
{
  "ConfigurationAggregator": {
    "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-xz2upuu6",
    "CreationTime": 1517952090.769,
    "ConfigurationAggregatorName": "MyAggregator",
    "AccountAggregationSources": [
      {
        "AllAwsRegions": true,
        "AccountIds": [
          "AccountID1",
          "AccountID2",
          "AccountID3",
          "AccountID4"
        ]
      }
    ]
  }
}
```

```
    ]
  },
  "LastUpdatedTime": 1517952566.445
}
}
```

OR

#### For an organization

```
{
  "ConfigurationAggregator": {
    "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floppus3",
    "CreationTime": 1517942461.442,
    "ConfigurationAggregatorName": "MyAggregator",
    "OrganizationAggregationSource": {
      "AllAwsRegions": true,
      "RoleArn": "arn:aws:config:Region:AccountID:config-aggregator/config-
aggregator-floppus3"
    },
    "LastUpdatedTime": 1517942461.442
  }
}
```

## Delete an Aggregator

### To delete a configuration aggregator using the AWS CLI

- Type the following command:

```
aws configservice delete-configuration-aggregator --configuration-aggregator-name
MyAggregator
```

If successful, the command executes with no additional output.

## Learn More

- [Concepts \(p. 2\)](#)
- [Authorizing Aggregator Accounts to Collect AWS Config Configuration and Compliance Data Using the AWS Command Line Interface \(p. 3275\)](#)
- [Viewing Compliance Data in the Aggregator Dashboard \(p. 3264\)](#)
- [Troubleshooting for Multi-Account Multi-Region Data Aggregation \(p. 3277\)](#)

# Authorizing Aggregator Accounts to Collect AWS Config Configuration and Compliance Data Using the Console

AWS Config allows you to authorize aggregator accounts to collect AWS Config configuration and compliance data.

This flow is not required if you are aggregating source accounts that are part of AWS Organizations.

On the **Authorizations** page, you can do the following:

- Add Authorization to allow an aggregator account and region to collect AWS Config configuration and compliance data.
- Authorize a pending request from an aggregator account to collect AWS Config configuration and compliance data.
- Delete an authorization for an aggregator account.

## Topics

- [Add Authorization for Aggregator Accounts and Regions \(p. 3274\)](#)
- [Authorize a Pending Request for an Aggregator Account \(p. 3275\)](#)
- [Delete Authorization for an Existing Aggregator Account \(p. 3275\)](#)
- [Learn More \(p. 3266\)](#)

## Add Authorization for Aggregator Accounts and Regions

You can add authorization to grant permission to aggregator accounts and regions to collect AWS Config configuration and compliance data.

1. Sign in to the AWS Management Console and open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. Navigate to the **Authorizations** page and choose **Add authorization**.
3. For **Aggregator account**, type the 12-digit account ID of an aggregator account.
4. For **Aggregator region**, choose the AWS regions where aggregator account is allowed to collect AWS Config configuration and compliance data.
5. Choose **Add authorization** to confirm your selection.

AWS Config displays an aggregator account, region, and authorization status.

### Note

You can also add authorization to aggregator accounts and regions programmatically using AWS CloudFormation sample template. For more information, see [AWS::Config::AggregationAuthorization](#) in the *AWS CloudFormation user guide*.

## Authorize a Pending Request for an Aggregator Account

If you have a pending authorization request from an existing aggregator account you will see the request status on the **Authorizations** page. You can authorize a pending request from this page.

1. For the aggregator account you want to authorize, choose **Authorize** in the Actions column.  
A confirmation message is displayed to confirm you grant permission to an aggregator account and region for collecting AWS Config data.
2. Choose **Authorize** to grant this permission for an aggregator account and region.  
The authorization status changes from **Requesting for authorization** to **Authorized**.

## Delete Authorization for an Existing Aggregator Account

1. For the aggregator account you want to delete authorization, choose **Delete** in the Actions column.  
A warning message is displayed. When you delete this authorization, AWS Config data is not shared with an aggregator account.  
**Note**  
After authorization for an aggregator is deleted the data will remain in the aggregator account for up to 24 hours before being deleted.
2. Choose **Delete** to confirm your selection.  
The aggregator account is deleted.

## Learn More

- [Concepts \(p. 2\)](#)
- [Setting Up an Aggregator Using the Console \(p. 3266\)](#)
- [Viewing Compliance Data in the Aggregator Dashboard \(p. 3264\)](#)
- [Troubleshooting for Multi-Account Multi-Region Data Aggregation \(p. 3277\)](#)

# Authorizing Aggregator Accounts to Collect AWS Config Configuration and Compliance Data Using the AWS Command Line Interface

You can authorize aggregator accounts to collect AWS Config data from source accounts and delete aggregator accounts using the AWS Command Line Interface (AWS CLI). To use the AWS Management Console, see [Authorizing Aggregator Accounts to Collect AWS Config Configuration and Compliance Data Using the Console \(p. 3274\)](#).

The AWS CLI is a unified tool to manage your AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and use scripts to automate them.

To install the AWS CLI on your local machine, see [Installing the AWS CLI](#) in the *AWS CLI User Guide*.

If necessary, type `aws configure` to configure the AWS CLI to use an AWS Region where AWS Config aggregators are available.

### Topics

- [Add Authorization for Aggregator Accounts and Regions \(p. 3276\)](#)
- [Delete an Authorization Account \(p. 3276\)](#)
- [Learn More \(p. 3266\)](#)

## Add Authorization for Aggregator Accounts and Regions

1. Open a command prompt or a terminal window.
2. Type the following command:

```
aws configservice put-aggregation-authorization --authorized-account-id AccountID --  
authorized-aws-region Region
```

3. Press Enter.

You should see output similar to the following:

```
{  
  "AggregationAuthorization": {  
    "AuthorizedAccountId": "AccountID",  
    "AggregationAuthorizationArn": "arn:aws:config:Region:AccountID:aggregation-  
authorization/AccountID/Region",  
    "CreationTime": 1518116709.993,  
    "AuthorizedAwsRegion": "Region"  
  }  
}
```

## Delete an Authorization Account

### To delete an authorized account using the AWS CLI

- Type the following command:

```
aws configservice delete-aggregation-authorization --authorized-account-id AccountID  
--authorized-aws-region Region
```

If successful, the command executes with no additional output.

## Learn More

- [Concepts \(p. 2\)](#)
- [Setting Up an Aggregator Using the AWS Command Line Interface \(p. 3268\)](#)
- [Viewing Compliance Data in the Aggregator Dashboard \(p. 3264\)](#)
- [Troubleshooting for Multi-Account Multi-Region Data Aggregation \(p. 3277\)](#)

# Troubleshooting for Multi-Account Multi-Region Data Aggregation

AWS Config might not aggregate data from source accounts for one of the following reasons:

If this happens	Do this
AWS Config is not enabled in the source account for accounts within an Organization.	Enable AWS Config in the source account and authorize the aggregator account to collect data.
Authorization is not granted to an aggregator account.	Sign in to the source account and grant authorization to the aggregator account to collect AWS Config data.
There might be a temporary issue that is preventing data aggregation.	Data aggregation is subject to delays. Wait for a few minutes.

AWS Config might not aggregate data from an organization for one of the following reasons:

If this happens	Do this
AWS Config is unable to access your organization details due to invalid IAM role.	Create an IAM role or select a valid IAM role from the IAM role list.  <b>Note</b> If the IAM role is invalid for more than 24 hours, AWS Config deletes data for entire organization.
AWS Config service access is disabled in your organization.	You can enable integration between AWS Config and AWS Organizations through the <code>EnableAWSServiceAccess</code> API. If you choose <b>Add my organization</b> in console, AWS Config automatically enables the integration between AWS Config and AWS Organizations.
AWS Config is unable to access your organization details because all features is not enabled in your organization.	<a href="#">Enable all features</a> in AWS Organizations console.
Organizational changes such as adding an account, removing an account, enabling service access, and disabling service access are not updated in Middle East (Bahrain) and Asia Pacific (Hong Kong) regions immediately.	Organizational changes are subject to 2 hour delay. Wait for 2 hours to see all organization changes.

## Learn More

- [Concepts \(p. 2\)](#)
- [Setting Up an Aggregator Using the Console \(p. 3266\)](#)
- [Authorizing Aggregator Accounts to Collect AWS Config Configuration and Compliance Data Using the Console \(p. 3274\)](#)
- [Viewing Compliance Data in the Aggregator Dashboard \(p. 3264\)](#)

# Security in AWS Config

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from data centers and network architectures that are built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The [shared responsibility model](#) describes this as security *of* the cloud and security *in* the cloud:

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the [AWS Compliance Programs](#). To learn about the compliance programs that apply to AWS Config, see [AWS Services in Scope by Compliance Program](#).
- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company's requirements, and applicable laws and regulations.

This documentation helps you understand how to apply the shared responsibility model when using AWS Config. The following topics show you how to configure AWS Config to meet your security and compliance objectives.

## Topics

- [Data Protection in AWS Config \(p. 3278\)](#)
- [AWS Identity and Access Management \(p. 3279\)](#)
- [AWS managed policies for AWS Config \(p. 3299\)](#)
- [Logging and Monitoring in AWS Config \(p. 3307\)](#)
- [Using AWS Config with Interface Amazon VPC Endpoints \(p. 3318\)](#)
- [Incident Response in AWS Config \(p. 3319\)](#)
- [Compliance Validation for AWS Config \(p. 3319\)](#)
- [Resilience in AWS Config \(p. 3320\)](#)
- [Infrastructure Security in AWS Config \(p. 3320\)](#)
- [Security Best Practices for AWS Config \(p. 3320\)](#)

## Data Protection in AWS Config

The AWS [shared responsibility model](#) applies to data protection in AWS Config. As described in this model, AWS is responsible for protecting the global infrastructure that runs all of the AWS Cloud. You are responsible for maintaining control over your content that is hosted on this infrastructure. This content includes the security configuration and management tasks for the AWS services that you use. For more information about data privacy, see the [Data Privacy FAQ](#). For information about data protection in Europe, see the [AWS Shared Responsibility Model and GDPR](#) blog post on the [AWS Security Blog](#).

For data protection purposes, we recommend that you protect AWS account credentials and set up individual user accounts with AWS Identity and Access Management (IAM). That way each user is given only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:

- Use multi-factor authentication (MFA) with each account.
- Use SSL/TLS to communicate with AWS resources. We recommend TLS 1.2 or later.
- Set up API and user activity logging with AWS CloudTrail.
- Use AWS encryption solutions, along with all default security controls within AWS services.
- Use advanced managed security services such as Amazon Macie, which assists in discovering and securing personal data that is stored in Amazon S3.
- If you require FIPS 140-2 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see [Federal Information Processing Standard \(FIPS\) 140-2](#).

We strongly recommend that you never put sensitive identifying information, such as your customers' account numbers, into free-form fields such as a **Name** field. This includes when you work with AWS Config or other AWS services using the console, API, AWS CLI, or AWS SDKs. Any data that you enter into AWS Config or other services might get picked up for inclusion in diagnostic logs. When you provide a URL to an external server, don't include credentials information in the URL to validate your request to that server.

## Encryption of Data at Rest

Data is encrypted at rest using transparent server-side encryption. This helps reduce the operational burden and complexity involved in protecting sensitive data. With encryption at rest, you can build security-sensitive applications that meet encryption compliance and regulatory requirements.

## Encryption of Data in Transit

Data gathered and accessed by AWS Config is exclusively over a Transport Layer Security (TLS) protected channel.

# AWS Identity and Access Management

AWS Config integrates with AWS Identity and Access Management (IAM), which allows you to create permission policies to attach to your IAM role, Amazon S3 buckets and Amazon Simple Notification Service (Amazon SNS) topics. You can use AWS Identity and Access Management to create AWS Config permission policies to attach to the IAM roles. A policy is a set of statements that grants AWS Config permissions.

### Important

We consider it a best practice not to use root account credentials to perform everyday work in AWS. Instead, we recommend that you create an IAM administrators group with appropriate permissions, create IAM users for the people in your organization who need to perform administrative tasks (including for yourself), and add those users to the administrative group. For more information, see [IAM Best Practices](#) in the *IAM User Guide* guide.

The first two topics control user permissions for AWS Config followed by topics that provide accurate configuration information about permissions needed for AWS Config. The topics provide examples of recommended IAM policies to use with the AWS Config console and the AWS Command Line Interface.

### Topics

- [Granting Permissions for AWS Config Administration \(p. 3280\)](#)
- [Granting Custom Permissions for AWS Config Users \(p. 3281\)](#)
- [Supported Resource-Level Permissions for AWS Config Rules APIs Actions \(p. 3287\)](#)
- [Permissions for the IAM Role Assigned to AWS Config \(p. 3289\)](#)

- [Permissions for the Amazon S3 Bucket \(p. 3292\)](#)
- [Permissions for the KMS Key \(p. 3294\)](#)
- [Permissions for the Amazon SNS Topic \(p. 3295\)](#)
- [Service-Linked AWS Config Rules \(p. 3297\)](#)

## Granting Permissions for AWS Config Administration

To allow users to administer AWS Config, you must grant explicit permissions to IAM users to perform the actions associated with AWS Config tasks. For most scenarios, you can do this using an AWS managed policy that contains predefined permissions.

### Note

The permissions you grant to users to perform AWS Config administration tasks are not the same as the permissions that AWS Config itself requires in order to deliver log files to Amazon S3 buckets or send notifications to Amazon SNS topics.

Users who set up and manage AWS Config must have full-access permissions. With full-access permissions, users can provide Amazon S3 and Amazon SNS endpoints that AWS Config delivers data to, create a role for AWS Config, and turn on and turn off recording.

Users who use AWS Config but don't need to set up AWS Config should have read-only permissions. With read-only permissions, users can look up the configurations of resources or search for resources by tags.

A typical approach is to create an IAM group that has the appropriate permissions and then add individual IAM users to that group. For example, you might create an IAM group for users who should have full access to AWS Config actions, and a separate group for users who should be able to view the configurations but not create or change a role.

### Contents

- [Creating an IAM Group and Users for AWS Config Access \(p. 3280\)](#)
- [Granting Full-Access Permission for AWS Config Access \(p. 3281\)](#)
- [Additional Resources \(p. 3281\)](#)

## Creating an IAM Group and Users for AWS Config Access

1. Open the IAM console at <https://console.aws.amazon.com/iam>.
2. From the dashboard, choose **Groups** in the navigation pane, and then choose **Create New Group**.
3. Type a name, and then choose **Next Step**.
4. On the **Attach Policy** page, find and choose **AWSConfigUserAccess**. This policy provides user access to use AWS Config, including searching by tags on resources, and reading all tags. This does not provide permission to configure AWS Config which requires administrative privileges.

### Note

You can also create a custom policy that grants permissions to individual actions. For more information, see [Granting Custom Permissions for AWS Config Users \(p. 3281\)](#).

5. Choose **Next Step**.
6. Review the information for the group you are about to create.

### Note

You can edit the group name, but you will need to choose the policy again.

7. Choose **Create Group**. The group that you created appears in the list of groups.
8. Choose the group name that you created, choose **Group Actions**, and then choose **Add Users to Group**.

9. On the **Add Users to Group** page, choose the existing IAM users, and then choose **Add Users**. If you don't already have IAM users, choose **Create New Users**, enter user names, and then choose **Create**.
10. If you created new users, choose **Users** in the navigation pane and complete the following for each user:
  - a. Choose the user.
  - b. If the user will use the console to manage AWS Config, in the **Security Credentials** tab, choose **Manage Password**, and then create a password for the user.
  - c. If the user will use the AWS CLI or API to manage AWS Config, and if you didn't already create access keys, in the **Security Credentials** tab, choose **Manage Access Keys** and then create access keys. Store the keys in a secure location.
  - d. Give each user his or her credentials (access keys or password).

## Granting Full-Access Permission for AWS Config Access

1. Sign in to the AWS Identity and Access Management (IAM) console at <https://console.aws.amazon.com/iam>.
2. In the navigation pane, choose **Policies**, and then choose **Create Policy**.
3. For **Create Your Own Policy**, choose **Select**.
4. Type a policy name and description. For example: `AWSConfigFullAccess`.
5. For **Policy Document**, type or paste the full-access policy into the editor. You can use the [Full access \(p. 3283\)](#).
6. Choose **Validate Policy** and ensure that no errors display in a red box at the top of the screen. Correct any errors that are reported.
7. Choose **Create Policy** to save your new policy.
8. In the list of policies, select the policy that you created. You can use the **Filter** menu and the **Search** box to find the policy.
9. Choose **Policy Actions**, and then choose **Attach**.
10. Select the users, groups, or roles, and then choose **Attach Policy**. You can use the **Filter** menu and the **Search** box to filter the list.
11. Choose **Apply Policy**.

### Note

Instead of creating a managed policy, you can also create an inline policy from the IAM console and attach it to an IAM user, group, or role. For more information, see [Working with Inline Policies](#) in the *IAM User Guide*.

## Additional Resources

To learn more about creating IAM users, groups, policies, and permissions, see [Creating an Admins Group Using the Console](#) and [Permissions and Policies](#) in the *IAM User Guide*.

## Granting Custom Permissions for AWS Config Users

AWS Config policies grant permissions to users who work with AWS Config. If you need to grant different permissions to users, you can attach a AWS Config policy to an IAM group or to a user. You can edit the policy to include or exclude specific permissions. You can also create your own custom policy. Policies are JSON documents that define the actions a user is allowed to perform and the resources that the user is allowed to perform those actions on.

### Contents

- [Read-only access \(p. 3282\)](#)
- [Full access \(p. 3283\)](#)
- [Controlling User Permissions for Actions on Multi-Account Multi-Region Data Aggregation \(p. 3284\)](#)
- [Additional Information \(p. 3281\)](#)

## Read-only access

The following example shows a AWS managed policy, `AWSConfigUserAccess` that grants read-only access to AWS Config.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "config:Get*",
        "config:Describe*",
        "config:Deliver*",
        "config:List*",
        "tag:GetResources",
        "tag:GetTagKeys",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents"
      ],
      "Resource": "*"
    }
  ]
}
```

In the policy statements, the `Effect` element specifies whether the actions are allowed or denied. The `Action` element lists the specific actions that the user is allowed to perform. The `Resource` element lists the AWS resources the user is allowed to perform those actions on. For policies that control access to AWS Config actions, the `Resource` element is always set to `*`, a wildcard that means "all resources."

The values in the `Action` element correspond to the APIs that the services support. The actions are preceded by `config:` to indicate that they refer to AWS Config actions. You can use the `*` wildcard character in the `Action` element, such as in the following examples:

- `"Action": ["config:*ConfigurationRecorder"]`

This allows all AWS Config actions that end with `ConfigurationRecorder` (`StartConfigurationRecorder`, `StopConfigurationRecorder`).

- `"Action": ["config:*"]`

This allows all AWS Config actions, but not actions for other AWS services.

- `"Action": ["*"]`

This allows all AWS actions. This permission is suitable for a user who acts as an AWS administrator for your account.

The read-only policy doesn't grant user permission for the actions such as `StartConfigurationRecorder`, `StopConfigurationRecorder`, and `DeleteConfigurationRecorder`. Users with this policy are not allowed to start configuration recorder, stop configuration recorder, or delete configuration recorder. For the list of AWS Config actions, see the [AWS Config API Reference](#).

## Full access

The following example shows a policy that grants full access to AWS Config. It grants users the permission to perform all AWS Config actions. It also lets users manage files in Amazon S3 buckets and manage Amazon SNS topics in the account that the user is associated with.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sns:AddPermission",
        "sns:CreateTopic",
        "sns>DeleteTopic",
        "sns:GetTopicAttributes",
        "sns:ListPlatformApplications",
        "sns:ListTopics",
        "sns:SetTopicAttributes"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:CreateBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketNotification",
        "s3:GetBucketPolicy",
        "s3:GetBucketRequestPayment",
        "s3:GetBucketVersioning",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:ListBucketVersions",
        "s3:PutBucketPolicy"
      ],
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:PassRole",
        "iam:PutRolePolicy",
        "iam:AttachRolePolicy",
        "iam:CreatePolicy",
        "iam:CreatePolicyVersion",
        "iam>DeletePolicyVersion",
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents"
      ]
    }
  ]
}
```

```
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "config:*",
      "tag:Get*"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "ssm:DescribeDocument",
      "ssm:GetDocument",
      "ssm:DescribeAutomationExecutions",
      "ssm:GetAutomationExecution",
      "ssm:ListDocuments",
      "ssm:StartAutomationExecution"
    ],
    "Resource": "*"
  }
]
}
```

**Note**

This policy grants broad permissions. Before granting full access, consider starting with a minimum set of permissions and granting additional permissions as necessary. Doing so is better practice than starting with permissions that are too lenient and then trying to tighten them later.

## Controlling User Permissions for Actions on Multi-Account Multi-Region Data Aggregation

You can use resource-level permissions to control a user's ability to perform specific actions on multi-account multi-region data aggregation. AWS Config multi-account multi-region data aggregation APIs support resource level permissions. With resource level permission can restrict to access/modify the resource data to specific users.

For example, you want to restrict access to resource data to specific users. You can create two aggregators `AccessibleAggregator` and `InAccessibleAggregator`. Then attach an IAM policy that allows access to the `AccessibleAggregator`.

In the first policy, you allow the aggregator actions such as `DescribeConfigurationAggregators` and `DeleteConfigurationAggregator` actions for the config ARN that you specify. In the following example, the config ARN is `arn:aws:config:ap-northeast-1:AccountID:config-aggregator/config-aggregator-mocpsqhs`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ConfigReadOnly",
      "Effect": "Allow",
      "Action": [
        "config:PutConfigurationAggregator",
        "config:DescribePendingAggregationRequests",
        "config>DeletePendingAggregationRequest",
```

```
        "config:GetAggregateConfigRuleComplianceSummary",
        "config:DescribeAggregateComplianceByConfigRules",
        "config:GetAggregateComplianceDetailsByConfigRule",
        "config:DescribeConfigurationAggregators",
        "config:DescribeConfigurationAggregatorSourcesStatus",
        "config>DeleteConfigurationAggregator"
    ],
    "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-aggregator/config-
aggregator-mocpsqhs"
}
]
}
```

In the second policy, you deny the aggregator actions for the config ARN that you specify. In the following example, the config ARN is `arn:aws:config:ap-northeast-1:AccountID:config-aggregator/config-aggregator-pokxzldx`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ConfigReadOnly",
      "Effect": "Deny",
      "Action": [
        "config:PutConfigurationAggregator",
        "config:DescribePendingAggregationRequests",
        "config>DeletePendingAggregationRequest",
        "config:GetAggregateConfigRuleComplianceSummary",
        "config:DescribeAggregateComplianceByConfigRules",
        "config:GetAggregateComplianceDetailsByConfigRule",
        "config:DescribeConfigurationAggregators",
        "config:DescribeConfigurationAggregatorSourcesStatus",
        "config>DeleteConfigurationAggregator"
      ],
      "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-aggregator/config-
aggregator-pokxzldx"
    }
  ]
}
```

If a user of the developer group tries to describe or delete configuration aggregators on the config that you specified in the second policy, that user gets an access denied exception.

The following AWS CLI examples show that the user creates two aggregators, `AccessibleAggregator` and `InAccessibleAggregator`.

```
aws configservice describe-configuration-aggregators
```

The command complete successfully:

```
{
  "ConfigurationAggregators": [
    {
      "ConfigurationAggregatorArn": "arn:aws:config:ap-northeast-1:AccountID:config-
aggregator/config-aggregator-mocpsqhs",
      "CreationTime": 1517942461.442,
      "ConfigurationAggregatorName": "AccessibleAggregator",
      "AccountAggregationSources": [
        {
          "AllAwsRegions": true,
```

```
        "AccountIDs": [
            "AccountID1",
            "AccountID2",
            "AccountID3"
        ]
    },
    ],
    "LastUpdatedTime": 1517942461.455
}
]
```

```
{
  "ConfigurationAggregators": [
    {
      "ConfigurationAggregatorArn": "arn:aws:config:ap-northeast-1:AccountID:config-
aggregator/config-aggregator-pokxzldx",
      "CreationTime": 1517942461.442,
      "ConfigurationAggregatorName": "InAccessibleAggregator",
      "AccountAggregationSources": [
        {
          "AllAwsRegions": true,
          "AccountIDs": [
            "AccountID1",
            "AccountID2",
            "AccountID3"
          ]
        }
      ],
      "LastUpdatedTime": 1517942461.455
    }
  ]
}
```

**Note**

For `account-aggregation-sources` enter a comma-separated list of AWS account IDs for which you want to aggregate data. Wrap the account IDs in square brackets, and be sure to escape quotation marks (for example, "[{\\"AccountIDs\\": [\\"AccountID1\\", \\"AccountID2\\", \\"AccountID3\\"], \\"AllAwsRegions\\": true}]").

The user then creates an IAM policy that denies access to `InAccessibleAggregator`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ConfigReadOnly",
      "Effect": "Deny",
      "Action": [
        "config:PutConfigurationAggregator",
        "config:DescribePendingAggregationRequests",
        "config>DeletePendingAggregationRequest",
        "config:GetAggregateConfigRuleComplianceSummary",
        "config:DescribeAggregateComplianceByConfigRules",
        "config:GetAggregateComplianceDetailsByConfigRule",
        "config:DescribeConfigurationAggregators",
        "config:DescribeConfigurationAggregatorSourcesStatus",
        "config>DeleteConfigurationAggregator"
      ],
      "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-aggregator/config-
aggregator-pokxzldx"
    }
  ]
}
```

```
]
}
```

Next, the user confirms that IAM policy works for restricting access to specific aggregator and rules.

```
aws configservice get-aggregate-compliance-details-by-config-rule --configuration-
aggregator-name InAccessibleAggregator --config-rule-name rule name --account-id AccountID
--aws-region AwsRegion
```

The command returns an access denied exception:

```
An error occurred (AccessDeniedException) when calling the
GetAggregateComplianceDetailsByConfigRule operation: User: arn:aws:iam::AccountID:user/ is
not
authorized to perform: config:GetAggregateComplianceDetailsByConfigRule on resource:
arn:aws:config:AwsRegion-1:AccountID:config-aggregator/config-aggregator-pokxzldx
```

With resource-level permissions, you can grant or deny access to perform specific actions on multi-account multi-region data aggregation.

## Additional Information

To learn more about creating IAM users, groups, policies, and permissions, see [Creating Your First IAM User and Administrators Group](#) and [Access Management](#) in the *IAM User Guide*.

# Supported Resource-Level Permissions for AWS Config Rules APIs Actions

Resource-level permissions refers to the ability to specify which resources users are allowed to perform actions on. AWS Config supports resource-level permissions for certain AWS Config Rules API actions. This means that for certain AWS Config Rules actions, you can control when users are allowed to use those actions based on conditions that have to be fulfilled, or specific resources that users are allowed to use.

The following table describes the AWS Config Rules API actions that currently support resource-level permissions, as well as the supported resources (and their ARNs) for each action. When specifying an ARN, you can use the \* wildcard in your paths; for example, when you cannot or do not want to specify exact resource IDs.

### Important

If an AWS Config Rules API action is not listed in this table, then it does not support resource-level permissions. If an AWS Config Rules action does not support resource-level permissions, you can grant users permissions to use the action, but you have to specify a \* for the resource element of your policy statement.

API Action	Resources
DeleteConfigRule	Config Rule arn:aws:config: <i>region</i> : <i>accountID</i> :config-rule/config-rule- <i>ID</i>
DeleteEvaluationResults	Config Rule arn:aws:config: <i>region</i> : <i>accountID</i> :config-rule/config-rule- <i>ID</i>
DescribeComplianceByConfigRule	Config Rule

AWS Config Developer Guide  
Supported Resource-Level Permissions  
for AWS Config Rules APIs Actions

API Action	Resources
	arn:aws:config: <i>region</i> : <i>accountID</i> :config-rule/config-rule- <i>ID</i>
DescribeConfigRuleEvaluationStatus	Config Rule arn:aws:config: <i>region</i> : <i>accountID</i> :config-rule/config-rule- <i>ID</i>
DescribeConfigRules	Config Rule arn:aws:config: <i>region</i> : <i>accountID</i> :config-rule/config-rule- <i>ID</i>
GetComplianceDetailsByConfigRule	Config Rule arn:aws:config: <i>region</i> : <i>accountID</i> :config-rule/config-rule- <i>ID</i>
PutConfigRule	Config Rule arn:aws:config: <i>region</i> : <i>accountID</i> :config-rule/config-rule- <i>ID</i>
StartConfigRulesEvaluation	Config Rule arn:aws:config: <i>region</i> : <i>accountID</i> :config-rule/config-rule- <i>ID</i>
PutRemediationConfigurations	Remediation Configuration arn:aws:config: <i>region</i> : <i>accountID</i> :remediation-configuration/ <i>config rule name/remediation configuration id</i>
DescribeRemediationConfigurations	Remediation Configuration arn:aws:config: <i>region</i> : <i>accountID</i> :remediation-configuration/ <i>config rule name/remediation configuration id</i>
DeleteRemediationConfiguration	Remediation Configuration arn:aws:config: <i>region</i> : <i>accountID</i> :remediation-configuration/ <i>config rule name/remediation configuration id</i>
PutRemediationExceptions	Remediation Configuration arn:aws:config: <i>region</i> : <i>accountID</i> :remediation-configuration/ <i>config rule name/remediation configuration id</i>
DescribeRemediationExceptions	Remediation Configuration arn:aws:config: <i>region</i> : <i>accountID</i> :remediation-configuration/ <i>config rule name/remediation configuration id</i>
DeleteRemediationExceptions	Remediation Configuration arn:aws:config: <i>region</i> : <i>accountID</i> :remediation-configuration/ <i>config rule name/remediation configuration id</i>

For example, you want to allow read access and deny write access to specific rules to specific users.

In the first policy, you allow the AWS Config Rules read actions such as `DescribeConfigRules` and `DescribeConfigRuleEvaluationStatus` on the specified rules.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "config:DescribeConfigRules",
        "config:StartConfigRulesEvaluation",
        "config:DescribeComplianceByConfigRule",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:GetComplianceDetailsByConfigRule"
      ],
      "Resource": [
        "arn:aws:config:region:accountID:config-rule/config-rule-ID",
        "arn:aws:config:region:accountID:config-rule/config-rule-ID"
      ]
    }
  ]
}
```

In the second policy, you deny the AWS Config Rules write actions on the specific rule.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Deny",
      "Action": [
        "config:PutConfigRule",
        "config>DeleteConfigRule",
        "config>DeleteEvaluationResults"
      ],
      "Resource": "arn:aws:config:region:accountID:config-rule/config-rule-ID"
    }
  ]
}
```

With resource-level permissions, you can allow read access and deny write access to perform specific actions on AWS Config Rules API actions.

## Permissions for the IAM Role Assigned to AWS Config

An AWS Identity and Access Management (IAM) role lets you define a set of permissions. AWS Config assumes the role that you assign to it to write to your S3 bucket, publish to your SNS topic, and to make `Describe` or `List` API requests to get configuration details for your AWS resources. For more information on IAM roles, see [IAM Roles](#) in the *IAM User Guide*.

When you use the AWS Config console to create or update an IAM role, AWS Config automatically attaches the required permissions for you. For more information, see [Setting Up AWS Config with the Console \(p. 25\)](#).

### Contents

- [Creating IAM Role Policies \(p. 3290\)](#)

- [Adding an IAM Trust Policy to your Role \(p. 3290\)](#)
- [IAM Role Policy for Amazon S3 Bucket \(p. 3290\)](#)
- [IAM Role Policy for KMS Key \(p. 3291\)](#)
- [IAM Role Policy for Amazon SNS Topic \(p. 3291\)](#)
- [IAM Role Policy for Getting Configuration Details \(p. 3291\)](#)
- [Managing Permissions for S3 Bucket Recording \(p. 3292\)](#)

## Creating IAM Role Policies

When you use the AWS Config console to create an IAM role, AWS Config automatically attaches the required permissions to the role for you.

If you are using the AWS CLI to set up AWS Config or you are updating an existing IAM role, you must manually update the policy to allow AWS Config to access your S3 bucket, publish to your SNS topic, and get configuration details about your resources.

### Adding an IAM Trust Policy to your Role

You can create an IAM trust policy that enables AWS Config to assume a role and use it to track your resources. For more information about trust policies, see [Assuming a Role](#) in the *IAM User Guide*.

The following is an example trust policy for AWS Config roles:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

### IAM Role Policy for Amazon S3 Bucket

The following example policy grants AWS Config permissions to access your Amazon S3 bucket:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource": [
        "arn:aws:s3:::myBucketName/prefix/AWSLogs/myAccountID/*"
      ],
      "Condition": {
        "StringLike": {
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    }
  ]
}
```

```
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:GetBucketAcl"
    ],
    "Resource": "arn:aws:s3:::myBucketName"
  }
]
```

## IAM Role Policy for KMS Key

The following example policy grants AWS Config permissions to use KMS-based encryption on new objects for S3 bucket delivery:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "myKMSKeyARN"
    }
  ]
}
```

## IAM Role Policy for Amazon SNS Topic

The following example policy grants AWS Config permissions to access your SNS topic:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sns:Publish",
      "Resource": "mySNSTopicARN"
    }
  ]
}
```

If your SNS topic is encrypted for additional setup instructions, see [Configuring AWS KMS Permissions](#) in the *Amazon Simple Notification Service Developer Guide*.

## IAM Role Policy for Getting Configuration Details

To record your AWS resource configurations, AWS Config requires IAM permissions to get the configuration details about your resources.

Use the AWS managed policy **AWS\_ConfigRole** and attach it to the IAM role that you assign to AWS Config. AWS updates this policy each time AWS Config adds support for an AWS resource type, which means AWS Config will continue to have the required permissions to get configuration details as long as the role has this managed policy attached.

If you create or update a role with the console, AWS Config attaches the **AWS\_ConfigRole** for you.

If you use the AWS CLI, use the `attach-role-policy` command and specify the Amazon Resource Name (ARN) for **AWS\_ConfigRole**:

```
$ aws iam attach-role-policy --role-name myConfigRole --policy-arn arn:aws:iam::aws:policy/service-role/AWS_ConfigRole
```

## Managing Permissions for S3 Bucket Recording

AWS Config records and delivers notifications when an S3 bucket is created, updated, or deleted.

It's recommended that you use either the `AWSServiceRoleForConfig` (see [Using Service-Linked Roles for AWS Config](#)) or a custom IAM role utilizing the `AWS_ConfigRole` managed policy. For more information on best practices for configuration recording, see [AWS Config Best Practices](#).

If you need to manage object-level permissions for your bucket recording, make sure in the S3 bucket policy to provide `config.amazonaws.com` (the AWS Config service principal name) access to all S3 related permissions from the `AWS_ConfigRole` managed policy. For more information, see [Permissions for the Amazon S3 Bucket](#).

## Permissions for the Amazon S3 Bucket

By default, all Amazon S3 buckets and objects are private. Only the resource owner which is the AWS account that created the bucket can access that bucket. The resource owner can, however, choose to grant access permissions to other resources and users. One way to do this is to write an access policy.

If AWS Config creates an Amazon S3 bucket for you automatically (for example, if you use AWS Config console to set up your delivery channel), these permissions are automatically added to Amazon S3 bucket. However, if you specify an existing Amazon S3 bucket, you must ensure that the S3 bucket has the correct permissions.

### Note

An object does not inherit the permissions from its bucket. For example, if you create a bucket and grant write access to a user, you can't access that user's objects unless the user explicitly grants you access.

### Contents

- [Required Permissions for the Amazon S3 Bucket When Using IAM Roles \(p. 3292\)](#)
- [Required Permissions for the Amazon S3 Bucket When Using Service-Linked Roles \(p. 3293\)](#)
- [Granting AWS Config access to the Amazon S3 Bucket \(p. 3293\)](#)

## Required Permissions for the Amazon S3 Bucket When Using IAM Roles

When AWS Config sends configuration information (history files and snapshots) to Amazon S3 bucket in your account, it assumes the IAM role that you assigned when you set up AWS Config. When AWS Config sends configuration information to an Amazon S3 bucket in another account, it first attempts to use the IAM role, but this attempt fails if the access policy for the bucket does not grant `WRITE` access to the IAM role. In this event, AWS Config sends the information again, this time as the AWS Config service principal. Before the delivery can succeed, the access policy must grant `WRITE` access to the `config.amazonaws.com` principal name. AWS Config is then the owner of the objects it delivers to the S3 bucket. You must attach an access policy, mentioned in step 6 below to the Amazon S3 bucket in another account to grant AWS Config access to the Amazon S3 bucket.

Before AWS Config can deliver logs to your Amazon S3 bucket AWS Config checks whether the bucket exists and in which AWS region the bucket is located. AWS Config attempts to call Amazon S3 [HeadBucket](#) API to check whether the bucket exists and to get the bucket region. If permissions are not provided to locate the bucket when the location check is performed, you see `AccessDenied` error in AWS CloudTrail logs. However, the log delivery to your Amazon S3 bucket succeeds if you do not provide bucket location permissions.

## Required Permissions for the Amazon S3 Bucket When Using Service-Linked Roles

If you set up AWS Config using a service-linked role, you need to attach an access policy, mentioned in step 6 below to the Amazon S3 bucket in your own account or another account to grant AWS Config access to the Amazon S3 bucket.

### Granting AWS Config access to the Amazon S3 Bucket

Follow these steps to add an access policy to the Amazon S3 bucket in your own account or another account. The access policy allows AWS Config to send configuration information to the Amazon S3 bucket.

1. Sign in to the AWS Management Console using the account that has the S3 bucket.
2. Open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
3. Select the bucket that you want AWS Config to use to deliver configuration items, and then choose **Properties**.
4. Choose **Permissions**.
5. Choose **Edit Bucket Policy**.
6. Copy the following policy into the **Bucket Policy Editor** window:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "config.amazonaws.com"
        ]
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::targetBucketName"
    },
    {
      "Sid": "AWSConfigBucketExistenceCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "config.amazonaws.com"
        ]
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::targetBucketName"
    },
    {
      "Sid": "AWSConfigBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "Service": [
```

```
        "config.amazonaws.com"
      ]
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::targetBucketName/[optional] prefix/
AWSLogs/sourceAccountID-WithoutHyphens/Config/*",
    "Condition": {
      "StringEquals": {
        "s3:x-amz-acl": "bucket-owner-full-control"
      }
    }
  }
}
]
```

#### Note

AWS Config is owned by AWS and does not belong specifically to one of your AWS accounts or linked accounts within your AWS Organization. This means that the service won't work with organization ID or organization units based conditions.

#### Note

When granting permissions to your IAM role instead of AWS Config service principal name (SPN), ensure that your IAM role has `PutObjectACL` permission on cross-account bucket to avoid insufficient permission error. See sample IAM role policy at [IAM Role Policy for Amazon S3 Bucket](#) (p. 3290).

7. Substitute the following values in the bucket policy:
  - `targetBucketName` – The name of the Amazon S3 bucket to which AWS Config will deliver configuration items.
  - `[optional] prefix` – An optional addition to the Amazon S3 object key that helps create a folder-like organization in the bucket.
  - `sourceAccountID-WithoutHyphens` – The ID of the account for which AWS Config will deliver configuration items to the target bucket.
8. Choose **Save** and then **Close**.

## Permissions for the KMS Key

Create a policy for an Amazon S3 KMS Key that allows you to use KMS-based encryption on objects delivered by AWS Config for S3 bucket delivery.

#### Contents

- [Required Permissions for the KMS Key When Using IAM Roles \(S3 Bucket Delivery\)](#) (p. 3294)
- [Required Permissions for the KMS Key When Using Service-Linked Roles \(S3 Bucket Delivery\)](#) (p. 3295)

## Required Permissions for the KMS Key When Using IAM Roles (S3 Bucket Delivery)

If you set up AWS Config using an IAM role, you can attach the follow permission policy to the KMS Key:

```
{
  "Id": "Policy_ID",
  "Statement": [
```

```
{
  "Sid": "AWSConfigKMSPolicy",
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Effect": "Allow",
  "Resource": "*myKMSKeyARN*",
  "Principal": {
    "AWS": [
      "account-id1",
      "account-id2",
      "account-id3"
    ]
  }
}
```

## Required Permissions for the KMS Key When Using Service-Linked Roles (S3 Bucket Delivery)

If you set up AWS Config using a service-linked role, you need to attach the following permission policy to the KMS Key.

```
{
  "Id": "Policy_ID",
  "Statement": [
    {
      "Sid": "AWSConfigKMSPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "myKMSKeyARN"
    }
  ]
}
```

## Permissions for the Amazon SNS Topic

Use the information in this topic only if you want to configure AWS Config to deliver Amazon SNS topics owned by your account or by a different account. AWS Config must have permissions to send notifications to an Amazon SNS topic.

### Note

AWS Config currently only supports same region and cross account access. SNS topics used for remediation AWS Systems Manager documents (SSM documents) or for the recorder delivery channel cannot be cross-region.

### Contents

- [Required Permissions for the Amazon SNS Topic When Using IAM Roles \(p. 3296\)](#)
- [Required Permissions for the Amazon SNS Topic When Using Service-Linked Roles \(p. 3296\)](#)

- [Troubleshooting for the Amazon SNS Topic \(p. 3297\)](#)

## Required Permissions for the Amazon SNS Topic When Using IAM Roles

You can attach a permission policy to the Amazon SNS topic owned by a different account. If you want to use an Amazon SNS topic from another account, make sure to attach the following policy to an existing Amazon SNS topic.

```
{
  "Id": "Policy1415489375392",
  "Statement": [
    {
      "Sid": "AWSConfigSNSPolicy20150201",
      "Action": [
        "SNS:Publish"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:sns:region:account-id:myTopic",
      "Principal": {
        "AWS": [
          "account-id1",
          "account-id2",
          "account-id3"
        ]
      }
    }
  ]
}
```

For the Resource key, *account-id* is the account number of the topic owner. For *account-id1*, *account-id2*, and *account-id3*, use the AWS accounts that will send data to an Amazon SNS topic. You must substitute appropriate values for *region* and *myTopic*.

## Required Permissions for the Amazon SNS Topic When Using Service-Linked Roles

If you set up AWS Config using a service-linked role, you need to attach a permission policy to the Amazon SNS topic. If you want to use an Amazon SNS topic from your own account, make sure to attach the following policy to an existing Amazon SNS topic.

```
{
  "Id": "Policy_ID",
  "Statement": [
    {
      "Sid": "AWSConfigSNSPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account-id:myTopic"
    }
  ]
}
```

You must substitute appropriate values for *region*, *account-id*, and *myTopic*.

## Troubleshooting for the Amazon SNS Topic

AWS Config must have permissions to send notifications to an Amazon SNS topic. If an Amazon SNS topic cannot receive notifications, verify that the IAM role that AWS Config was assuming must have `sns:publish` permissions.

## Service-Linked AWS Config Rules

A service-linked AWS Config rule is a unique type of managed config rule that supports other AWS services to create AWS Config rules in your account. The service-linked AWS Config rules are predefined to include all the permissions required to call other AWS services on your behalf. These rules are similar to standards that an AWS service recommends in your AWS account for compliance verification.

These service-linked AWS Config rules are owned by AWS service teams. The AWS service team creates these rules in your AWS account. You have read-only access to these rules. You cannot edit or delete these rules if you are subscribed to AWS service that these rules are linked to.

In the AWS Config console, the service-linked AWS Config rules are visible in the **Rules** page. The edit button is greyed in the console thereby restricting you to edit the rule. You can view details of the rule by choosing the rule. On the rule details page, you can view the name of the service that created the rule. The **Edit** and **Delete results** is greyed thereby restricting you to edit and delete results of the rule. To edit or delete the rule, contact the AWS service that created the rule.

While using the AWS Command Line Interface, the `PutConfigRule`, `DeleteConfigRule`, and `DeleteEvaluationResults` APIs return access denied with the following error message:

```
INSUFFICIENT_SLCR_PERMISSIONS = "An AWS service owns ServiceLinkedConfigRule.  
You do not have permissions to take action on this rule."
```

### Topics

- [Using Service-Linked Roles for AWS Config \(p. 3297\)](#)

## Using Service-Linked Roles for AWS Config

AWS Config uses AWS Identity and Access Management (IAM) [service-linked roles](#). A service-linked role is a unique type of IAM role that is linked directly to AWS Config. Service-linked roles are predefined by AWS Config and include all the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up AWS Config easier because you don't have to manually add the necessary permissions. AWS Config defines the permissions of its service-linked roles, and unless defined otherwise, only AWS Config can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

For information about other services that support service-linked roles, see [AWS Services That Work with IAM](#) and look for the services that have **Yes** in the **Service-Linked Role** column. Choose a **Yes** with a link to view the service-linked role documentation for that service.

## Service-Linked Role Permissions for AWS Config

AWS Config uses the service-linked role named **AWSServiceRoleForConfig** – AWS Config uses this service-linked role to call other AWS services on your behalf.

The **AWSServiceRoleForConfig** service-linked role trusts the `config.amazonaws.com` service to assume the role.

The permissions policy for the **AWSServiceRoleForConfig** role contains read-only and write-only permissions for AWS Config resources and read-only permissions for resources in other services that AWS Config supports. For more information, see [Supported Resource Types \(p. 9\)](#).

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see [Service-Linked Role Permissions](#) in the *IAM User Guide*.

To use a service-linked role with AWS Config, you must configure permissions on your Amazon S3 bucket and Amazon SNS topic. For more information, see [Required Permissions for the Amazon S3 Bucket When Using Service-Linked Roles \(p. 3293\)](#) and [Required Permissions for the Amazon SNS Topic When Using Service-Linked Roles \(p. 3296\)](#).

## Creating a Service-Linked Role for AWS Config

In the IAM CLI or the IAM API, create a service-linked role with the `config.amazonaws.com` service name. For more information, see [Creating a Service-Linked Role](#) in the *IAM User Guide*. If you delete this service-linked role, you can use this same process to create the role again.

## Editing a Service-Linked Role for AWS Config

AWS Config does not allow you to edit the **AWSServiceRoleForConfig** service-linked role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see [Editing a Service-Linked Role](#) in the *IAM User Guide*.

## Deleting a Service-Linked Role for AWS Config

If you no longer need to use a feature or service that requires a service-linked role, we recommend that you delete that role. That way you don't have an unused entity that is not actively monitored or maintained. However, you must clean up the resources for your service-linked role before you can manually delete it.

### Note

If the AWS Config service is using the role when you try to delete the resources, then the deletion might fail. If that happens, wait for a few minutes and try the operation again.

### To delete AWS Config resources used by the **AWSServiceRoleForConfig**

Ensure that you do not have `ConfigurationRecorders` using the service-linked role. You can use the AWS Config console to stop the configuration recorder. To stop recording, under **Recording is on**, choose **Turn off**.

You can delete the `ConfigurationRecorder` using AWS Config API. To delete, use the `delete-configuration-recorder` command.

```
$ aws configservice delete-configuration-recorder --configuration-recorder-name default
```

### To manually delete the service-linked role using IAM

Use the IAM console, the IAM CLI, or the IAM API to delete the **AWSServiceRoleForConfig** service-linked role. For more information, see [Deleting a Service-Linked Role](#) in the *IAM User Guide*.

## AWS managed policies for AWS Config

To add permissions to users, groups, and roles, it is easier to use AWS managed policies than to write policies yourself. It takes time and expertise to [create IAM customer managed policies](#) that provide your team with only the permissions they need. To get started quickly, you can use our AWS managed policies. These policies cover common use cases and are available in your AWS account. For more information about AWS managed policies, see [AWS managed policies](#) in the *IAM User Guide*.

AWS services maintain and update AWS managed policies. You can't change the permissions in AWS managed policies. Services occasionally add additional permissions to an AWS managed policy to support new features. This type of update affects all identities (users, groups, and roles) where the policy is attached. Services are most likely to update an AWS managed policy when a new feature is launched or when new operations become available. Services do not remove permissions from an AWS managed policy, so policy updates won't break your existing permissions.

Additionally, AWS supports managed policies for job functions that span multiple services. For example, the **ReadOnlyAccess** AWS managed policy provides read-only access to all AWS services and resources. When a service launches a new feature, AWS adds read-only permissions for new operations and resources. For a list and descriptions of job function policies, see [AWS managed policies for job functions](#) in the *IAM User Guide*.

### AWS managed policy: AWSConfigServiceRolePolicy

AWS Config uses the service-linked role named **AWSServiceRoleForConfig** to call other AWS services on your behalf. When you use AWS Management Console to set up AWS Config, this SLR is automatically created by AWS Config if you select the option to use the AWS Config SLR instead of your own AWS Identity and Access Management (IAM) service role.

The **AWSServiceRoleForConfig** SLR contains the managed policy **AWSConfigServiceRolePolicy**. This managed policy contains read-only and write-only permissions for AWS Config resources and read-only permissions for resources in other services that AWS Config supports. For more information, see [Supported Resource Types \(p. 9\)](#) and [Using Service-Linked Roles for AWS Config \(p. 3297\)](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm:ListTagsForCertificate",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeTags",
        "backup:ListBackupPlans",
        "backup:GetBackupPlan",
        "backup:ListBackupVaults",
        "backup:DescribeBackupVault",
        "backup:GetBackupVaultNotifications",
        "backup:GetBackupVaultAccessPolicy",
        "backup:ListBackupSelections",
        "backup:GetBackupSelection",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:DescribeRecoveryPoint",

```

```
"backup:ListTags",
"cloudfront:ListTagsForResource",
"cloudformation:DescribeType",
"cloudformation:ListTypes",
"cloudtrail:DescribeTrails",
"cloudtrail:GetEventSelectors",
"cloudtrail:GetTrailStatus",
"cloudtrail:ListTags",
"cloudwatch:DescribeAlarms",
"codepipeline:GetPipeline",
"codepipeline:GetPipelineState",
"codepipeline:ListPipelines",
"config:BatchGet*",
"config:Describe*",
"config:Get*",
"config:List*",
"config:Put*",
"config>Select*",
"dax:DescribeClusters",
"dms:DescribeReplicationInstances",
"dms:DescribeReplicationSubnetGroups",
"dms:ListTagsForResource",
"dynamodb:DescribeContinuousBackups",
"dynamodb:DescribeLimits",
"dynamodb:DescribeTable",
"dynamodb:ListTables",
"dynamodb:ListTagsOfResource",
"ec2:Describe*",
"ec2:GetEbsEncryptionByDefault",
"ecr:DescribeRepositories",
"ecr:GetLifecyclePolicy",
"ecr:GetRepositoryPolicy",
"ecr:ListTagsForResource",
"ecs:DescribeClusters",
"ecs:DescribeServices",
"ecs:DescribeTaskDefinition",
"ecs:DescribeTaskSets",
"ecs:ListClusters",
"ecs:ListServices",
"ecs:ListTagsForResource",
"ecs:ListTaskDefinitions",
"eks:DescribeCluster",
"eks:DescribeNodegroup",
"eks:ListClusters",
"eks:ListNodegroups",
"elasticache:DescribeCacheClusters",
"elasticache:DescribeCacheParameterGroups",
"elasticache:DescribeCacheSubnetGroups",
"elasticache:DescribeReplicationGroups",
"elasticfilesystem:DescribeAccessPoints",
"elasticfilesystem:DescribeBackupPolicy",
"elasticfilesystem:DescribeFileSystems",
"elasticfilesystem:DescribeFileSystemPolicy",
"elasticfilesystem:DescribeLifecycleConfiguration",
"elasticfilesystem:DescribeMountTargets",
"elasticfilesystem:DescribeMountTargetSecurityGroups",
"elasticloadbalancing:DescribeListeners",
"elasticloadbalancing:DescribeLoadBalancerAttributes",
"elasticloadbalancing:DescribeLoadBalancerPolicies",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeRules",
"elasticloadbalancing:DescribeTags",
"elasticmapreduce:DescribeCluster",
"elasticmapreduce:DescribeSecurityConfiguration",
"elasticmapreduce:GetBlockPublicAccessConfiguration",
"elasticmapreduce:ListClusters",
```

```
"elasticmapreduce:ListInstances",
"es:DescribeElasticsearchDomain",
"es:DescribeElasticsearchDomains",
"es:ListDomainNames",
"es:ListTags",
"guardduty:GetDetector",
"guardduty:GetFindings",
"guardduty:GetMasterAccount",
"guardduty:ListDetectors",
"guardduty:ListFindings",
"iam:GenerateCredentialReport",
"iam:GetAccountAuthorizationDetails",
"iam:GetAccountPasswordPolicy",
"iam:GetAccountSummary",
"iam:GetCredentialReport",
"iam:GetGroup",
"iam:GetGroupPolicy",
"iam:GetPolicy",
"iam:GetPolicyVersion",
"iam:GetRole",
"iam:GetRolePolicy",
"iam:GetUser",
"iam:GetUserPolicy",
"iam:ListAttachedGroupPolicies",
"iam:ListAttachedRolePolicies",
"iam:ListAttachedUserPolicies",
"iam:ListEntitiesForPolicy",
"iam:ListGroupPolicies",
"iam:ListGroupsForUser",
"iam:ListInstanceProfilesForRole",
"iam:ListPolicyVersions",
"iam:ListRolePolicies",
"iam:ListUserPolicies",
"iam:ListVirtualMFADevices",
"kinesis:DescribeStreamSummary",
"kinesis:ListStreams",
"kinesis:ListTagsForStream",
"kms:DescribeKey",
"kms:GetKeyPolicy",
"kms:GetKeyRotationStatus",
"kms:ListKeys",
"kms:ListResourceTags",
"lambda:GetAlias",
"lambda:GetFunction",
"lambda:GetPolicy",
"lambda:ListAliases",
"lambda:ListFunctions",
"logs:DescribeLogGroups",
"organizations:DescribeOrganization",
"rds:DescribeDBClusters",
"rds:DescribeDBClusterSnapshotAttributes",
"rds:DescribeDBClusterSnapshots",
"rds:DescribeDBInstances",
"rds:DescribeDBSecurityGroups",
"rds:DescribeDBSnapshotAttributes",
"rds:DescribeDBSnapshots",
"rds:DescribeDBSubnetGroups",
"rds:DescribeEventSubscriptions",
"rds:ListTagsForResource",
"redshift:DescribeClusterParameterGroups",
"redshift:DescribeClusterParameters",
"redshift:DescribeClusterSecurityGroups",
"redshift:DescribeClusterSnapshots",
"redshift:DescribeClusterSubnetGroups",
"redshift:DescribeClusters",
"redshift:DescribeEventSubscriptions",
```

```

    "redshift:DescribeLoggingStatus",
    "route53:GetHostedZone",
    "route53:ListHostedZones",
    "route53:ListHostedZonesByName",
    "route53:ListResourceRecordSets",
    "route53:ListTagsForResource",
    "s3:GetAccelerateConfiguration",
    "s3:GetAccessPoint",
    "s3:GetAccountPublicAccessBlock",
    "s3:GetBucketAcl",
    "s3:GetBucketCORS",
    "s3:GetBucketLocation",
    "s3:GetBucketLogging",
    "s3:GetBucketNotification",
    "s3:GetBucketObjectLockConfiguration",
    "s3:GetBucketPolicy",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketRequestPayment",
    "s3:GetBucketTagging",
    "s3:GetBucketVersioning",
    "s3:GetBucketWebsite",
    "s3:GetEncryptionConfiguration",
    "s3:GetLifecycleConfiguration",
    "s3:GetReplicationConfiguration",
    "s3:ListAccessPoints",
    "s3:ListAllMyBuckets",
    "s3:ListBucket",
    "sagemaker:DescribeCodeRepository",
    "sagemaker:DescribeEndpointConfig",
    "sagemaker:DescribeNotebookInstance",
    "sagemaker:ListCodeRepositories",
    "sagemaker:ListEndpointConfigs",
    "sagemaker:ListNotebookInstances",
    "sagemaker:ListTags",
    "secretsmanager:ListSecrets",
    "secretsmanager:ListSecretVersionIds",
    "securityhub:describeHub",
    "shield:DescribeDRTAccess",
    "shield:DescribeProtection",
    "shield:DescribeSubscription",
    "sns:GetTopicAttributes",
    "sns:ListSubscriptions",
    "sns:ListTagsForResource",
    "sns:ListTopics",
    "sqs:GetQueueAttributes",
    "sqs:ListQueues",
    "sqs:ListQueueTags",
    "ssm:DescribeAutomationExecutions",
    "ssm:DescribeDocument",
    "ssm:GetAutomationExecution",
    "ssm:GetDocument",
    "ssm:ListDocuments",
    "storagegateway:ListGateways",
    "storagegateway:ListVolumes",
    "support:DescribeCases",
    "tag:GetResources",
    "waf:GetLoggingConfiguration",
    "waf:GetWebACL",
    "wafv2:GetLoggingConfiguration",
    "waf-regional:GetLoggingConfiguration",
    "waf-regional:GetWebACL",
    "waf-regional:GetWebACLForResource"
  ],
  "Resource": "*"
}
]

```

```
}
```

## AWS managed policy: AWS\_ConfigRole

If you want to create an IAM role for AWS Config, use the managed policy `AWS_ConfigRole` and attach it to your IAM role.

This IAM policy is updated each time AWS Config adds support for an AWS resource type. This means that AWS Config will continue to have the required permissions to record configuration data of supported resource types as long as the **AWS\_ConfigRole** role has this managed policy attached. For more information, see [Supported Resource Types \(p. 9\)](#) and [Permissions for the IAM Role Assigned to AWS Config \(p. 3289\)](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm:ListTagsForCertificate",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeTags",
        "backup:ListBackupPlans",
        "backup:GetBackupPlan",
        "backup:ListBackupVaults",
        "backup:DescribeBackupVault",
        "backup:GetBackupVaultNotifications",
        "backup:GetBackupVaultAccessPolicy",
        "backup:ListBackupSelections",
        "backup:GetBackupSelection",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:DescribeRecoveryPoint",
        "backup:ListTags",
        "cloudfront:ListTagsForResource",
        "cloudformation:DescribeType",
        "cloudformation:ListTypes",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:ListTags",
        "cloudwatch:DescribeAlarms",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:ListPipelines",
        "config:BatchGet*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:Put*",
        "config>Select*",
        "dax:DescribeClusters",
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationSubnetGroups",
        "dms:ListTagsForResource",
        "dynamodb:DescribeContinuousBackups",
```

```
"dynamodb:DescribeLimits",
"dynamodb:DescribeTable",
"dynamodb:ListTables",
"dynamodb:ListTagsOfResource",
"ec2:Describe*",
"ec2:GetEbsEncryptionByDefault",
"ecr:DescribeRepositories",
"ecr:GetLifecyclePolicy",
"ecr:GetRepositoryPolicy",
"ecr:ListTagsForResource",
"ecs:DescribeClusters",
"ecs:DescribeServices",
"ecs:DescribeTaskDefinition",
"ecs:DescribeTaskSets",
"ecs:ListClusters",
"ecs:ListServices",
"ecs:ListTagsForResource",
"ecs:ListTaskDefinitions",
"eks:DescribeCluster",
"eks:DescribeNodegroup",
"eks:ListClusters",
"eks:ListNodegroups",
"elasticache:DescribeCacheClusters",
"elasticache:DescribeCacheParameterGroups",
"elasticache:DescribeCacheSubnetGroups",
"elasticache:DescribeReplicationGroups",
"elasticfilesystem:DescribeAccessPoints",
"elasticfilesystem:DescribeBackupPolicy",
"elasticfilesystem:DescribeFileSystems",
"elasticfilesystem:DescribeFileSystemPolicy",
"elasticfilesystem:DescribeLifecycleConfiguration",
"elasticfilesystem:DescribeMountTargets",
"elasticfilesystem:DescribeMountTargetSecurityGroups",
"elasticloadbalancing:DescribeListeners",
"elasticloadbalancing:DescribeLoadBalancerAttributes",
"elasticloadbalancing:DescribeLoadBalancerPolicies",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeRules",
"elasticloadbalancing:DescribeTags",
"elasticmapreduce:DescribeCluster",
"elasticmapreduce:DescribeSecurityConfiguration",
"elasticmapreduce:GetBlockPublicAccessConfiguration",
"elasticmapreduce:ListClusters",
"elasticmapreduce:ListInstances",
"es:DescribeElasticsearchDomain",
"es:DescribeElasticsearchDomains",
"es:ListDomainNames",
"es:ListTags",
"guardduty:GetDetector",
"guardduty:GetFindings",
"guardduty:GetMasterAccount",
"guardduty:ListDetectors",
"guardduty:ListFindings",
"iam:GenerateCredentialReport",
"iam:GetAccountAuthorizationDetails",
"iam:GetAccountPasswordPolicy",
"iam:GetAccountSummary",
"iam:GetCredentialReport",
"iam:GetGroup",
"iam:GetGroupPolicy",
"iam:GetPolicy",
"iam:GetPolicyVersion",
"iam:GetRole",
"iam:GetRolePolicy",
"iam:GetUser",
"iam:GetUserPolicy",
```

```
"iam:ListAttachedGroupPolicies",
"iam:ListAttachedRolePolicies",
"iam:ListAttachedUserPolicies",
"iam:ListEntitiesForPolicy",
"iam:ListGroupPolicies",
"iam:ListGroupsForUser",
"iam:ListInstanceProfilesForRole",
"iam:ListPolicyVersions",
"iam:ListRolePolicies",
"iam:ListUserPolicies",
"iam:ListVirtualMFADevices",
"kinesis:DescribeStreamSummary",
"kinesis:ListStreams",
"kinesis:ListTagsForStream",
"kms:DescribeKey",
"kms:GetKeyPolicy",
"kms:GetKeyRotationStatus",
"kms:ListKeys",
"kms:ListResourceTags",
"lambda:GetAlias",
"lambda:GetFunction",
"lambda:GetPolicy",
"lambda:ListAliases",
"lambda:ListFunctions",
"logs:DescribeLogGroups",
"organizations:DescribeOrganization",
"rds:DescribeDBClusters",
"rds:DescribeDBClusterSnapshotAttributes",
"rds:DescribeDBClusterSnapshots",
"rds:DescribeDBInstances",
"rds:DescribeDBSecurityGroups",
"rds:DescribeDBSnapshotAttributes",
"rds:DescribeDBSnapshots",
"rds:DescribeDBSubnetGroups",
"rds:DescribeEventSubscriptions",
"rds:ListTagsForResource",
"redshift:DescribeClusterParameterGroups",
"redshift:DescribeClusterParameters",
"redshift:DescribeClusterSecurityGroups",
"redshift:DescribeClusterSnapshots",
"redshift:DescribeClusterSubnetGroups",
"redshift:DescribeClusters",
"redshift:DescribeEventSubscriptions",
"redshift:DescribeLoggingStatus",
"route53:GetHostedZone",
"route53:ListHostedZones",
"route53:ListHostedZonesByName",
"route53:ListResourceRecordSets",
"route53:ListTagsForResource",
"s3:GetAccelerateConfiguration",
"s3:GetAccessPoint",
"s3:GetAccountPublicAccessBlock",
"s3:GetBucketAcl",
"s3:GetBucketCORS",
"s3:GetBucketLocation",
"s3:GetBucketLogging",
"s3:GetBucketNotification",
"s3:GetBucketObjectLockConfiguration",
"s3:GetBucketPolicy",
"s3:GetBucketPublicAccessBlock",
"s3:GetBucketRequestPayment",
"s3:GetBucketTagging",
"s3:GetBucketVersioning",
"s3:GetBucketWebsite",
"s3:GetEncryptionConfiguration",
"s3:GetLifecycleConfiguration",
```

```

"s3:GetReplicationConfiguration",
"s3:ListAccessPoints",
"s3:ListAllMyBuckets",
"s3:ListBucket",
"sagemaker:DescribeCodeRepository",
"sagemaker:DescribeEndpointConfig",
"sagemaker:DescribeNotebookInstance",
"sagemaker:ListCodeRepositories",
"sagemaker:ListEndpointConfigs",
"sagemaker:ListNotebookInstances",
"sagemaker:ListTags",
"secretsmanager:ListSecrets",
"secretsmanager:ListSecretVersionIds",
"securityhub:describeHub",
"shield:DescribeDRTAccess",
"shield:DescribeProtection",
"shield:DescribeSubscription",
"sns:GetTopicAttributes",
"sns:ListSubscriptions",
"sns:ListTagsForResource",
"sns:ListTopics",
"sqs:GetQueueAttributes",
"sqs:ListQueues",
"sqs:ListQueueTags",
"ssm:DescribeAutomationExecutions",
"ssm:DescribeDocument",
"ssm:GetAutomationExecution",
"ssm:GetDocument",
"ssm:ListDocuments",
"storagegateway:ListGateways",
"storagegateway:ListVolumes",
"support:DescribeCases",
>tag:GetResources",
"waf:GetLoggingConfiguration",
"waf:GetWebACL",
"wafv2:GetLoggingConfiguration",
"waf-regional:GetLoggingConfiguration",
"waf-regional:GetWebACL",
"waf-regional:GetWebACLForResource"
],
"Resource": "*"
}
]
}

```

## AWS Config updates to AWS managed policies

View details about updates to AWS managed policies for AWS Config since this service began tracking these changes. For automatic alerts about changes to this page, subscribe to the RSS feed on the AWS Config [Document history](#) page.

Change	Description	Date
<a href="#">AWSConfigServiceRolePolicy (p. 327)</a> – Add ssm:ListDocuments permission and additional permissions for new resource types	This policy now grants permission to view information about AWS Systems Manager (formerly known as SSM) specified documents. This policy also now supports additional AWS resource types for AWS Backup, Amazon Elastic File	April 1, 2021

Change	Description	Date
	System, Amazon ElastiCache, Amazon Simple Storage Service, Amazon Elastic Compute Cloud, Amazon Kinesis, Amazon SageMaker, AWS Database Migration Service, and Amazon Route 53. These permission changes allow AWS Config to invoke the read-only APIs required to support these resource types.	
<a href="#">AWS_ConfigRole (p. 3303)</a> – Add <code>ssm:ListDocuments</code> permission and additional permissions for new resource types	This policy now grants permission to view information about AWS Systems Manager (formerly known as SSM) specified documents. This policy also now supports additional AWS resource types for AWS Backup, Amazon Elastic File System, Amazon ElastiCache, Amazon Simple Storage Service, Amazon Elastic Compute Cloud, Amazon Kinesis, Amazon SageMaker, AWS Database Migration Service, and Amazon Route 53. These permission changes allow AWS Config to invoke the read-only APIs required to support these resource types.	April 1, 2021
AWS Config started tracking changes	AWS Config started tracking changes for its AWS managed policies.	April 1, 2021

## Logging and Monitoring in AWS Config

AWS Config is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in AWS Config. Monitoring is an important part of maintaining the reliability, availability, and performance of AWS Config and your AWS solutions.

### Logging AWS Config API Calls with AWS CloudTrail

CloudTrail captures all API calls for AWS Config as events. The calls captured include calls from the AWS Config console and code calls to the AWS Config API operations. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for AWS Config. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in **Event history**. Using the information collected by CloudTrail, you can determine the request that was made to AWS Config, the IP address from which the request was made, who made the request, when it was made, and additional details.

To learn more about CloudTrail, see the [AWS CloudTrail User Guide](#).

### Topics

- [AWS Config Information in CloudTrail \(p. 3308\)](#)
- [Understanding AWS Config Log File Entries \(p. 3308\)](#)
- [Example Log Files \(p. 3308\)](#)

## AWS Config Information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When activity occurs in AWS Config, that activity is recorded in a CloudTrail event along with other AWS service events in **Event history**. You can view, search, and download recent events in your AWS account. For more information, see [Viewing Events with CloudTrail Event History](#).

For an ongoing record of events in your AWS account, including events for AWS Config, create a trail. A *trail* enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all AWS Regions. The trail logs events from all Regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see the following:

- [Overview for Creating a Trail](#)
- [CloudTrail Supported Services and Integrations](#)
- [Configuring Amazon SNS Notifications for CloudTrail](#)
- [Receiving CloudTrail Log Files from Multiple Regions](#) and [Receiving CloudTrail Log Files from Multiple Accounts](#)

All AWS Config operations are logged by CloudTrail and are documented in the [AWS Config API Reference](#). For example, calls to the [DeliverConfigSnapshot](#), [DeleteDeliveryChannel](#), and [DescribeDeliveryChannels](#) operations generate entries in the CloudTrail log files.

Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root or AWS Identity and Access Management (IAM) user credentials.
- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another AWS service.

For more information, see the [CloudTrail userIdentity Element](#).

## Understanding AWS Config Log File Entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.

## Example Log Files

For examples of the CloudTrail log entries, see the following topics.

### Contents

- [DeleteDeliveryChannel](#) (p. 3309)
- [DeliverConfigSnapshot](#) (p. 3309)
- [DescribeConfigurationRecorderStatus](#) (p. 3310)
- [DescribeConfigurationRecorders](#) (p. 3310)
- [DescribeDeliveryChannels](#) (p. 3311)
- [GetResourceConfigHistory](#) (p. 3311)
- [PutConfigurationRecorder](#) (p. 3312)
- [PutDeliveryChannel](#) (p. 3313)
- [StartConfigurationRecorder](#) (p. 3313)
- [StopConfigurationRecorder](#) (p. 3314)

## DeleteDeliveryChannel

The following is an example CloudTrail log file for the operation.

```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::222222222222:user/JohnDoe",
    "accountId": "222222222222",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "JohnDoe"
  },
  "eventTime": "2014-12-11T18:32:57Z",
  "eventSource": "config.amazonaws.com",
  "eventName": "DeleteDeliveryChannel",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "10.24.34.0",
  "userAgent": "aws-internal/3",
  "requestParameters": {
    "deliveryChannelName": "default"
  },
  "responseElements": null,
  "requestID": "207d695a-8164-11e4-ab4f-657c7ab282ab",
  "eventID": "5dcff7a9-e414-411a-a43e-88d122a0ad4a",
  "eventType": "AwsApiCall",
  "recipientAccountId": "222222222222"
}
```

## DeliverConfigSnapshot

The following is an example CloudTrail log file for the operation.

```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDAABCDEFGHIJKLMNPOQ:Config-API-Test",
    "arn": "arn:aws:sts::111111111111:assumed-role/JaneDoe/Config-API-Test",
    "accountId": "111111111111",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2014-12-11T00:58:42Z"
      }
    }
  }
}
```

```
    },
    "sessionIssuer": {
      "type": "Role",
      "principalId": "AIDAABCDEFGHIJKLMOPQ",
      "arn": "arn:aws:iam::111111111111:role/JaneDoe",
      "accountId": "111111111111",
      "userName": "JaneDoe"
    }
  }
},
"eventTime": "2014-12-11T00:58:53Z",
"eventSource": "config.amazonaws.com",
"eventName": "DeliverConfigSnapshot",
"awsRegion": "us-west-2",
"sourceIPAddress": "10.24.34.0",
"userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
"requestParameters": {
  "deliveryChannelName": "default"
},
"responseElements": {
  "configSnapshotId": "58d50f10-212d-4fa4-842e-97c614da67ce"
},
"requestID": "e0248561-80d0-11e4-9f1c-7739d36a3df2",
"eventID": "3e88076c-ee1-4aa6-8990-86fe52aedbd8",
"eventType": "AwsApiCall",
"recipientAccountId": "111111111111"
}
```

## DescribeConfigurationRecorderStatus

The following is an example CloudTrail log file for the operation.

```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::222222222222:user/JohnDoe",
    "accountId": "222222222222",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "userName": "JohnDoe"
  },
  "eventTime": "2014-12-11T18:35:44Z",
  "eventSource": "config.amazonaws.com",
  "eventName": "DescribeConfigurationRecorderStatus",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
  "requestParameters": null,
  "responseElements": null,
  "requestID": "8442f25d-8164-11e4-ab4f-657c7ab282ab",
  "eventID": "a675b36b-455f-4e18-a4bc-d3e01749d3f1",
  "eventType": "AwsApiCall",
  "recipientAccountId": "222222222222"
}
```

## DescribeConfigurationRecorders

The following is an example CloudTrail log file for the operation.

```
{
  "eventVersion": "1.02",
```

```
"userIdentity": {
  "type": "IAMUser",
  "principalId": "AIDACKCEVSQ6C2EXAMPLE",
  "arn": "arn:aws:iam::222222222222:user/JohnDoe",
  "accountId": "222222222222",
  "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
  "userName": "JohnDoe"
},
"eventTime": "2014-12-11T18:34:52Z",
"eventSource": "config.amazonaws.com",
"eventName": "DescribeConfigurationRecorders",
"awsRegion": "us-west-2",
"sourceIPAddress": "192.0.2.0",
"userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
"requestParameters": null,
"responseElements": null,
"requestID": "6566b55c-8164-11e4-ab4f-657c7ab282ab",
"eventID": "6259a9ad-889e-423b-beeb-6e1eec84a8b5",
"eventType": "AwsApiCall",
"recipientAccountId": "222222222222"
}
```

## DescribeDeliveryChannels

Following is an example CloudTrail log file for the operation.

```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::222222222222:user/JohnDoe",
    "accountId": "222222222222",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "userName": "JohnDoe"
  },
  "eventTime": "2014-12-11T18:35:02Z",
  "eventSource": "config.amazonaws.com",
  "eventName": "DescribeDeliveryChannels",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
  "requestParameters": null,
  "responseElements": null,
  "requestID": "6b6aee3f-8164-11e4-ab4f-657c7ab282ab",
  "eventID": "3e15ebc5-bf39-4d2a-8b64-9392807985f1",
  "eventType": "AwsApiCall",
  "recipientAccountId": "222222222222"
}
```

## GetResourceConfigHistory

The following is an example CloudTrail log file for the operation.

```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDAABCDEFGHIJKLMNPOQ:Config-API-Test",
    "arn": "arn:aws:sts::111111111111:assumed-role/JaneDoe/Config-API-Test",
    "accountId": "111111111111",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",

```

```

"sessionContext": {
  "attributes": {
    "mfaAuthenticated": "false",
    "creationDate": "2014-12-11T00:58:42Z"
  },
  "sessionIssuer": {
    "type": "Role",
    "principalId": "AIDAABCDEFGHIJKLMOPQ",
    "arn": "arn:aws:iam::111111111111:role/JaneDoe",
    "accountId": "111111111111",
    "userName": "JaneDoe"
  }
},
"eventTime": "2014-12-11T00:58:42Z",
"eventSource": "config.amazonaws.com",
"eventName": "GetResourceConfigHistory",
"awsRegion": "us-west-2",
"sourceIPAddress": "10.24.34.0",
"userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
"requestParameters": {
  "resourceId": "vpc-a12bc345",
  "resourceType": "AWS::EC2::VPC",
  "limit": 0,
  "laterTime": "Dec 11, 2014 12:58:42 AM",
  "earlierTime": "Dec 10, 2014 4:58:42 PM"
},
"responseElements": null,
"requestID": "d9f3490d-80d0-11e4-9f1c-7739d36a3df2",
"eventID": "ba9c1766-d28f-40e3-b4c6-3ffb87dd6166",
"eventType": "AwsApiCall",
"recipientAccountId": "111111111111"
}

```

## PutConfigurationRecorder

The following is an example CloudTrail log file for the operation.

```

{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::222222222222:user/JohnDoe",
    "accountId": "222222222222",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "userName": "JohnDoe"
  },
  "eventTime": "2014-12-11T18:35:23Z",
  "eventSource": "config.amazonaws.com",
  "eventName": "PutConfigurationRecorder",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
  "requestParameters": {
    "configurationRecorder": {
      "name": "default",
      "roleARN": "arn:aws:iam::222222222222:role/config-role-pdx"
    }
  },
  "responseElements": null,
  "requestID": "779f7917-8164-11e4-ab4f-657c7ab282ab",
  "eventID": "c91f3daa-96e8-44ee-8ddd-146ac06565a7",
  "eventType": "AwsApiCall",
}

```

```
"recipientAccountId": "222222222222"  
}
```

## PutDeliveryChannel

The following is an example CloudTrail log file for the operation.

```
{  
  "eventVersion": "1.02",  
  "userIdentity": {  
    "type": "IAMUser",  
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",  
    "arn": "arn:aws:iam::222222222222:user/JohnDoe",  
    "accountId": "222222222222",  
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",  
    "userName": "JohnDoe"  
  },  
  "eventTime": "2014-12-11T18:33:08Z",  
  "eventSource": "config.amazonaws.com",  
  "eventName": "PutDeliveryChannel",  
  "awsRegion": "us-west-2",  
  "sourceIPAddress": "192.0.2.0",  
  "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",  
  "requestParameters": {  
    "deliveryChannel": {  
      "name": "default",  
      "s3BucketName": "config-api-test-pdx",  
      "snsTopicARN": "arn:aws:sns:us-west-2:222222222222:config-api-test-pdx"  
    }  
  },  
  "responseElements": null,  
  "requestID": "268b8d4d-8164-11e4-ab4f-657c7ab282ab",  
  "eventID": "b2db05f1-1c73-4e52-b238-db69c04e8dd4",  
  "eventType": "AwsApiCall",  
  "recipientAccountId": "222222222222"  
}
```

## StartConfigurationRecorder

The following is an example CloudTrail log file for the operation.

```
{  
  "eventVersion": "1.02",  
  "userIdentity": {  
    "type": "IAMUser",  
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",  
    "arn": "arn:aws:iam::222222222222:user/JohnDoe",  
    "accountId": "222222222222",  
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",  
    "userName": "JohnDoe"  
  },  
  "eventTime": "2014-12-11T18:35:34Z",  
  "eventSource": "config.amazonaws.com",  
  "eventName": "StartConfigurationRecorder",  
  "awsRegion": "us-west-2",  
  "sourceIPAddress": "192.0.2.0",  
  "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",  
  "requestParameters": {  
    "configurationRecorderName": "default"  
  },  
  "responseElements": null,  
  "requestID": "7e03fa6a-8164-11e4-ab4f-657c7ab282ab",  
}
```

```
"eventID": "55a5507f-f306-4896-afe3-196dc078a88d",  
"eventType": "AwsApiCall",  
"recipientAccountId": "222222222222"  
}
```

## StopConfigurationRecorder

The following is an example CloudTrail log file for the operation.

```
{  
  "eventVersion": "1.02",  
  "userIdentity": {  
    "type": "IAMUser",  
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",  
    "arn": "arn:aws:iam::222222222222:user/JohnDoe",  
    "accountId": "222222222222",  
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",  
    "userName": "JohnDoe"  
  },  
  "eventTime": "2014-12-11T18:35:13Z",  
  "eventSource": "config.amazonaws.com",  
  "eventName": "StopConfigurationRecorder",  
  "awsRegion": "us-west-2",  
  "sourceIPAddress": "192.0.2.0",  
  "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",  
  "requestParameters": {  
    "configurationRecorderName": "default"  
  },  
  "responseElements": null,  
  "requestID": "716deea3-8164-11e4-ab4f-657c7ab282ab",  
  "eventID": "6225a85d-1e49-41e9-bf43-3cfc5549e560",  
  "eventType": "AwsApiCall",  
  "recipientAccountId": "222222222222"  
}
```

## Monitoring

You can use other AWS services to monitor AWS Config resources.

- You can use Amazon Simple Notification Service (SNS) to send you notifications every time a supported AWS resource is created, updated, or otherwise modified as a result of user API activity.
- You can use Amazon CloudWatch Events to detect and react to changes in the status of AWS Config events.

### Topics

- [Monitoring AWS Resource Changes with Amazon SQS \(p. 3314\)](#)
- [Monitoring AWS Config with Amazon CloudWatch Events \(p. 3316\)](#)

## Monitoring AWS Resource Changes with Amazon SQS

AWS Config uses Amazon Simple Notification Service (SNS) to send you notifications every time a supported AWS resource is created, updated, or otherwise modified as a result of user API activity. However, you might be interested in only certain resource configuration changes. For example, you might consider it critical to know when someone modifies the configuration of a security group, but not need to know every time there is a change to tags on your Amazon EC2 instances. Or, you might want to write a program that performs specific actions when specific resources are updated. For example, you

might want to start a certain workflow when a security group configuration is changed. If you want to programmatically consume the data from AWS Config in these or other ways, use an Amazon Simple Queue Service queue as the notification endpoint for Amazon SNS.

**Note**

Notifications can also come from Amazon SNS in the form of an email, a Short Message Service (SMS) message to SMS-enabled mobile phones and smartphones, a notification message to an application on a mobile device, or a notification message to one or more HTTP or HTTPS endpoints.

You can have a single SQS queue subscribe to multiple topics, whether you have one topic per region or one topic per account per region. You must subscribe the queue to your desired SNS topic. (You can subscribe multiple queues to one SNS topic.) For more information, see [Sending Amazon SNS Messages to Amazon SQS Queues](#).

## Permissions for Amazon SQS

To use Amazon SQS with AWS Config, you must configure a policy that grants permissions to your account to perform all actions that are allowed on an SQS queue. The following example policy grants the account number 111122223333 and account number 444455556666 permission to send messages pertaining to each configuration change to the queue named `arn:aws:sqs:us-east-2:444455556666:queue1`.

```
{
  "Version": "2012-10-17",
  "Id": "Queue1_Policy_UUID",
  "Statement":
  {
    "Sid": "Queue1_SendMessage",
    "Effect": "Allow",
    "Principal": {
      "AWS": ["111122223333", "444455556666"]
    },
    "Action": "sqs:SendMessage",
    "Resource": "arn:aws:sqs:us-east-2:444455556666:queue1"
  }
}
```

You must also create a policy that grants permissions for connections between an SNS topic and the SQS queue that subscribes to that topic. The following is an example policy that permits the SNS topic with the Amazon Resource Name (ARN) `arn:aws:sns:us-east-2:111122223333:test-topic` to perform any actions on the queue named `arn:aws:sqs:us-east-2:111122223333:test-topic-queue`.

**Note**

The account for the SNS topic and the SQS queue must be in the same region.

```
{
  "Version": "2012-10-17",
  "Id": "SNSstoSQS",
  "Statement":
  {
    "Sid": "rule1",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "sqs:*",
    "Resource": "arn:aws:sqs:us-east-2:111122223333:test-topic-queue",
    "Condition": {
      "StringEquals": {
        "aws:SourceArn": "arn:aws:sns:us-east-2:111122223333:test-topic"
      }
    }
  }
}
```

```
}  
  }  
}
```

Each policy can include statements that cover only a single queue, not multiple queues. For information about other restrictions on Amazon SQS policies, see [Special Information for Amazon SQS Policies](#).

## Monitoring AWS Config with Amazon CloudWatch Events

### Note

Amazon EventBridge is the preferred way to manage your events. CloudWatch Events and EventBridge are the same underlying service and API, but EventBridge provides more features. Changes you make in either CloudWatch or EventBridge will appear in each console. For more information, see [Amazon EventBridge](#).

Amazon CloudWatch Events delivers a near real-time stream of system events that describe changes in AWS resources. Use Amazon CloudWatch Events to detect and react to changes in the status of AWS Config events.

You can create a rule that runs whenever there is a state transition, or when there is a transition to one or more states that are of interest. Then, based on rules you create, Amazon CloudWatch Events invokes one or more target actions when an event matches the values you specify in a rule. Depending on the type of event, you might want to send notifications, capture event information, take corrective action, initiate events, or take other actions.

Before you create event rules for AWS Config, however, you should do the following:

- Familiarize yourself with events, rules, and targets in CloudWatch Events. For more information, see [What Is Amazon CloudWatch Events?](#)
- For more information about how to get started with CloudWatch Events and set up rules, see [Getting Started with CloudWatch Events](#).
- Create the target or targets you will use in your event rules.

### Topics

- [Amazon CloudWatch Events format for AWS Config \(p. 3316\)](#)
- [Creating Amazon CloudWatch Events Rule for AWS Config \(p. 3317\)](#)

## Amazon CloudWatch Events format for AWS Config

The CloudWatch [event](#) for AWS Config has the following format:

```
{  
  "version": "0",  
  "id": "cd4d811e-ab12-322b-8255-872ce65b1bc8",  
  "detail-type": "event type",  
  "source": "aws.config",  
  "account": "111122223333",  
  "time": "2018-03-22T00:38:11Z",  
  "region": "us-east-1",  
  "resources": [resources],  
  "detail": {specific message type}  
}
```

## Creating Amazon CloudWatch Events Rule for AWS Config

Use the following steps to create a CloudWatch Events rule that triggers on an event emitted by AWS Config. Events are emitted on a best effort basis.

1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
2. In the navigation pane, choose **Events**.
3. Choose **Create rule**.
4. On the **Step 1: Create rule** page, for **Service Name**, choose **Config**.
5. For **Event Type**, choose the event type that triggers the rule:
  - Choose **All Events** to make a rule that applies to all AWS services. If you choose this option, you cannot choose specific message types, rule names, resource types, or resource IDs.
  - Choose **AWS API Call via CloudTrail** to base rules on API calls made to this service. For more information about creating this type of rule, see [Creating a CloudWatch Events Rule That Is Triggered on an AWS API Call Using AWS CloudTrail](#).
  - Choose **Config Configuration Item Change** to get notifications when a resource in your account changes.
  - Choose **Config Rules Compliance Change** to get notifications when a compliance check to your rules fails.
  - Choose **Config Rules Re-evaluation Status** to get reevaluation status notifications.
  - Choose **Config Configuration Snapshot Delivery Status** to get configuration snapshot delivery status notifications.
  - Choose **Config Configuration History Delivery Status** to get configuration history delivery status notifications.
6. Choose **Any message type** to receive notifications of any type. Choose **Specific message type(s)** to receive the following types of notifications:
  - If you choose **ConfigurationItemChangeNotification**, you receive messages when AWS Config successfully delivers the configuration snapshot to your Amazon S3 bucket.
  - If you choose **ComplianceChangeNotification**, you receive messages when the compliance type of a resource that AWS Config evaluates has changed.
  - If you choose **ConfigRulesEvaluationStarted**, you receive messages when AWS Config starts evaluating your rule against the specified resources.
  - If you choose **ConfigurationSnapshotDeliveryCompleted**, you receive messages when AWS Config successfully delivers the configuration snapshot to your Amazon S3 bucket.
  - If you choose **ConfigurationSnapshotDeliveryFailed**, you receive messages when AWS Config fails to deliver the configuration snapshot to your Amazon S3 bucket.
  - If you choose **ConfigurationSnapshotDeliveryStarted**, you receive messages when AWS Config starts delivering the configuration snapshot to your Amazon S3 bucket.
  - If you choose **ConfigurationHistoryDeliveryCompleted**, you receive messages when AWS Config successfully delivers the configuration history to your Amazon S3 bucket.
7. If you chose a specific event type from the **Event Type** drop-down list, choose **Any resource type** to make a rule that applies to all AWS Config supported resource types.

Or choose **Specific resource type(s)**, and then type the AWS Config supported resource type (for example, `AWS::EC2::Instance`).
8. If you chose a specific event type from the **Event Type** drop-down list, choose **Any resource ID** to include any AWS Config supported resource ID.

Or choose **Specific resource ID(s)**, and then type the AWS Config supported resource ID (for example, `i-04606de676e635647`).

9. If you chose a specific event type from the **Event Type** drop-down list, choose **Any rule name** to include any AWS Config supported rule.  
  
Or choose **Specific rule name(s)**, and then type the AWS Config supported rule (for example, **required-tags**).
- 10 Review your rule setup to make sure it meets your event-monitoring requirements.
- 11 In the **Targets** area, choose **Add target\***.
- 12 In the **Select target type** list, choose the type of target you have prepared to use with this rule, and then configure any additional options required by that type.
- 13 Choose **Configure details**.
- 14 On the **Configure rule details** page, type a name and description for the rule, and then choose the **State** box to enable the rule as soon as it is created.
- 15 Choose **Create rule** to confirm your selection.

## Using AWS Config with Interface Amazon VPC Endpoints

If you use Amazon Virtual Private Cloud (Amazon VPC) to host your AWS resources, you can establish a private connection between your VPC and AWS Config. You can use this connection to communicate with AWS Config from your VPC without going through the public internet.

Amazon VPC is an AWS service that you can use to launch AWS resources in a virtual network that you define. With a VPC, you have control over your network settings, such the IP address range, subnets, route tables, and network gateways. Interface VPC endpoints are powered by AWS PrivateLink, an AWS technology that enables private communication between AWS services using an elastic network interface with private IP addresses. To connect your VPC to AWS Config, you define an *interface VPC endpoint* for AWS Config. This type of endpoint enables you to connect your VPC to AWS services. The endpoint provides reliable, scalable connectivity to AWS Config without requiring an internet gateway, network address translation (NAT) instance, or VPN connection. For more information, see [What is Amazon VPC](#) in the *Amazon VPC User Guide*.

The following steps are for users of Amazon VPC. For more information, see [Getting Started](#) in the *Amazon VPC User Guide*.

### Availability

AWS Config currently supports VPC endpoints in the following Regions:

- US East (Ohio)
- US East (N. Virginia)
- US West (N. California)
- US West (Oregon)
- Asia Pacific (Mumbai)
- Asia Pacific (Seoul)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- Canada (Central)
- Europe (Frankfurt)
- Europe (Ireland)

- Europe (London)
- Europe (Paris)
- South America (São Paulo)
- Asia Pacific (Hong Kong)
- Africa (Cape Town)
- Europe (Milan)
- Europe (Stockholm)
- Middle East (Bahrain)
- AWS GovCloud (US-East)
- AWS GovCloud (US-West)

## Create a VPC Endpoint for AWS Config

To start using AWS Config with your VPC, create an interface VPC endpoint for AWS Config. You do not need to change the settings for AWS Config. AWS Config calls other AWS services using their public endpoints. For more information, see [Creating an Interface Endpoint](#) in the *Amazon VPC User Guide*.

## Incident Response in AWS Config

Incident response for AWS Config is an AWS responsibility. AWS has a formal, documented policy and program that governs incident response.

AWS operational issues with broad impact are posted on the AWS Service Health Dashboard. Operational issues are also posted to individual accounts via the Personal Health Dashboard.

## Compliance Validation for AWS Config

Third-party auditors assess the security and compliance of AWS Config as part of multiple AWS compliance programs. These include SOC, PCI, FedRAMP, HIPAA, and others.

For a list of AWS services in scope of specific compliance programs, see [AWS Services in Scope by Compliance Program](#). For general information, see [AWS Compliance Programs](#).

You can download third-party audit reports using AWS Artifact. For more information, see [Downloading Reports in AWS Artifact](#).

Your compliance responsibility when using AWS services is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. AWS provides the following resources to help with compliance:

- [Security and Compliance Quick Start Guides](#) – These deployment guides discuss architectural considerations and provide steps for deploying security- and compliance-focused baseline environments on AWS.
- [Architecting for HIPAA Security and Compliance Whitepaper](#) – This whitepaper describes how companies can use AWS to create HIPAA-compliant applications.

**Note**

Not all services are compliant with HIPAA.

- [AWS Compliance Resources](#) – This collection of workbooks and guides might apply to your industry and location.

- [Evaluating Resources with Rules](#) in the *AWS Config Developer Guide* – The AWS Config service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- [AWS Security Hub](#) – This AWS service provides a comprehensive view of your security state within AWS that helps you check your compliance with security industry standards and best practices.
- [AWS Audit Manager](#) – This AWS service helps you continuously audit your AWS usage to simplify how you manage risk and compliance with regulations and industry standards.

## Resilience in AWS Config

The AWS global infrastructure is built around AWS Regions and Availability Zones. AWS Regions provide multiple physically separated and isolated Availability Zones, which are connected with low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate applications and databases that automatically fail over between zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

For more information about AWS Regions and Availability Zones, see [AWS Global Infrastructure](#).

## Infrastructure Security in AWS Config

As a managed service, AWS Config is protected by the AWS global network security procedures that are described in the [Amazon Web Services: Overview of Security Processes](#) whitepaper.

You use AWS published API calls to access AWS Config through the network. Clients must support Transport Layer Security (TLS) 1.0 or later. We recommend TLS 1.2 or later. Clients must also support cipher suites with perfect forward secrecy (PFS) such as Ephemeral Diffie-Hellman (DHE) or Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Most modern systems such as Java 7 and later support these modes.

Additionally, requests must be signed by using an access key ID and a secret access key that is associated with an IAM principal. Or you can use the [AWS Security Token Service](#) (AWS STS) to generate temporary security credentials to sign requests.

## Configuration and Vulnerability Analysis

For AWS Config, AWS handles basic security tasks such as guest operating system (OS) and database patching, firewall configuration, and disaster recovery.

## Security Best Practices for AWS Config

AWS Config provides a number of security features to consider as you develop and implement your own security policies. The following best practices are general guidelines and don't represent a complete security solution. Because these best practices might not be appropriate or sufficient for your environment, treat them as helpful considerations rather than prescriptions.

- Leverage tagging for AWS Config, which makes it easier to manage, search for, and filter resources.
- Confirm your [delivery channels](#) have been properly set, and once confirmed, verify that AWS Config is [recording properly](#).

For more information, see [AWS Config best practices](#) blog.

# AWS Config Resources

The following related resources can help you as you work with this service.

- [AWS Config](#) – The primary web page for information about AWS Config.
- [AWS Config Pricing](#)
- [Technical FAQ](#)
- [Partners](#) – Links to partner products that are fully integrated with AWS Config to help you visualize, monitor, and manage the data from your configuration stream, configuration snapshots, or configuration history.
- [Classes & Workshops](#) – Links to role-based and specialty courses as well as self-paced labs to help sharpen your AWS skills and gain practical experience.
- [AWS Developer Tools](#) – Links to developer tools, SDKs, IDE toolkits, and command line tools for developing and managing AWS applications.
- [AWS Whitepapers](#) – Links to a comprehensive list of technical AWS whitepapers, covering topics such as architecture, security, and economics and authored by AWS Solutions Architects or other technical experts.
- [AWS Support Center](#) – The hub for creating and managing your AWS Support cases. Also includes links to other helpful resources, such as forums, technical FAQs, service health status, and AWS Trusted Advisor.
- [AWS Support](#) – The primary webpage for information about AWS Support, a one-on-one, fast-response support channel to help you build and run applications in the cloud.
- [Contact Us](#) – A central contact point for inquiries concerning AWS billing, account, events, abuse, and other issues.
- [AWS Site Terms](#) – Detailed information about our copyright and trademark; your account, license, and site access; and other topics.

## AWS Software Development Kits for AWS Config

An AWS software development kit (SDK) makes it easier to build applications that access cost-effective, scalable, and reliable AWS infrastructure services. With AWS SDKs, you can get started in minutes with a single, downloadable package that includes the library, code samples, and reference documentation. The following table lists the available SDKs and third-party libraries you can use to access AWS Config programmatically.

Type of Access	Description
AWS SDKs	<p>AWS provides the following SDKs:</p> <ul style="list-style-type: none"><li>• <a href="#">AWS SDK for C++ Documentation</a></li><li>• <a href="#">AWS Mobile SDK for iOS Documentation</a></li><li>• <a href="#">AWS SDK for Go Documentation</a></li><li>• <a href="#">AWS SDK for Java Documentation</a></li><li>• <a href="#">AWS SDK for JavaScript Documentation</a></li><li>• <a href="#">AWS SDK for .NET Documentation</a></li><li>• <a href="#">AWS SDK for PHP Documentation</a></li></ul>

Type of Access	Description
	<ul style="list-style-type: none"><li>• <a href="#">AWS SDK for Python (Boto) Documentation</a></li><li>• <a href="#">AWS SDK for Ruby Documentation</a></li></ul>
Third-party libraries	<p>Developers in the AWS developer community also provide their own libraries, which you can find at the following AWS developer centers:</p> <ul style="list-style-type: none"><li>• <a href="#">AWS Java Developer Center</a></li><li>• <a href="#">AWS JavaScript Developer Center</a></li><li>• <a href="#">AWS PHP Developer Center</a></li><li>• <a href="#">AWS Python Developer Center</a></li><li>• <a href="#">AWS Ruby Developer Center</a></li><li>• <a href="#">AWS Windows and .NET Developer Center</a></li></ul>

# Frequently Asked Questions

## Changes to AWS Config Resource Relationships

### Topics

- [What is the new change in the AWS Config Resource Relationships? \(p. 3323\)](#)
- [What is a direct and an in-direct relationship with respect to a resource? \(p. 3323\)](#)
- [What is the benefit of this change to AWS Config subscribers? \(p. 3324\)](#)
- [Which resource relationships are being removed? \(p. 3324\)](#)
- [How are the AWS Config managed rules affected? \(p. 3323\)](#)
- [What is the exact impact for custom AWS Config rules that use configuration trigger for these resource types? \(p. 3323\)](#)
- [Should I expect a delay in reporting evaluation results for a managed rule with configuration changes? \(p. 3323\)](#)
- [What is the impact on historical data? Would it still display details about indirect relationships? \(p. 3323\)](#)
- [Is there a change in the output generated by GetResourceConfigHistory API? \(p. 3323\)](#)
- [Is there any change in the resource schema of a Configuration Item? \(p. 3323\)](#)
- [Are there other alternatives to retrieve indirect relationships? \(p. 3323\)](#)

## What is the new change in the AWS Config Resource Relationships?

To optimize costs associated with recording changes related to ephemeral workloads, AWS Config will release an update to relationships modeled within ConfigurationItems (CI) for seven Amazon EC2 resource types on **August 1, 2021**. Examples of ephemeral workloads include changes to Amazon Elastic Compute Cloud (Amazon EC2) spot instances, Amazon Elastic MapReduce jobs, and Amazon EC2 autoscaling. This update optimized CI models for Amazon EC2 instance, security group, network interface, subnet, VPC, VPN gateway, and customer gateway resource types to record direct relationships and deprecate indirect relationships.

## What is a direct and an in-direct relationship with respect to a resource?

A direct relationship is defined as a one-way relationship (A->B) between a resource (A) and another resource (B), and is typically derived from the Describe API response of resource (A). An indirect relationship, on the other hand, is a relationship that AWS Config infers (B->A), in order to create a bidirectional relationship. For example, **Amazon EC2 instance -> Security Group** is a direct relationship, since security groups are returned as part of the describe API response for an Amazon EC2 instance. But **Security Group -> Amazon EC2 instance** is an indirect relationship, since Amazon EC2 instances are not returned when describing an Amazon EC2 Security group.

## What is the benefit of this change to AWS Config subscribers?

By deprecating indirect relationships, there are fewer configuration items related to relationship changes. This helps in containing AWS Config costs especially in case of ephemeral workloads, where there is a high volume of configuration changes for Amazon EC2 resource types.

## Which resource relationships are being removed?

The following resource relationships are deprecated.

Resource Type	Indirect Relationship With Resource Type		
AWS::EC2::CustomerGateway	AWS::VPN::Connection		
AWS::EC2::Instance	AWS::EC2::EIP, AWS::EC2::RouteTable		
AWS::EC2::NetworkInterface	AWS::EC2::EIP, AWS::EC2::RouteTable		
AWS::EC2::SecurityGroup	AWS::EC2::Instance, AWS::EC2::NetworkInterface		
AWS::EC2::Subnet	AWS::EC2::Instance, AWS::EC2::NetworkACL, AWS::EC2::NetworkInterface, AWS::EC2::RouteTable		
AWS::EC2::VPC	AWS::EC2::Instance, AWS::EC2::InternetGateway, AWS::EC2::NetworkACL, AWS::EC2::NetworkInterface, AWS::EC2::RouteTable, AWS::EC2::Subnet, AWS::EC2::VPNGateway, AWS::EC2::SecurityGroup		
AWS::EC2::VPNGateway	AWS::EC2::RouteTable, AWS::EC2::VPNConnection		

## How are the AWS Config managed rules affected?

AWS Config managed rules that trigger on one of the resources listed above, are updated by the AWS Config team. If you have not defined tags for these rules, no action is needed on your part. If tags are defined, you might need to make updates to the tags of your managed rules.

## What is the exact impact for custom AWS Config rules that use configuration trigger for these resource types?

If you use a custom rule that is not triggered by the resources listed in the above table, then no further action is required on your part. If you have a rule that triggers on one of the resources from the above table, examine the rule to determine if the Compliant status requires information from another resource whose relationship is listed in table. The change to the resource relationship will result in fewer changes being triggered since indirect relationships (listed in above table) will no longer be tracked. Add the related resources as an additional configuration trigger or use advanced queries if the information is essential to the implementation logic of your rule.

## Should I expect a delay in reporting evaluation results for a managed rule with configuration changes?

Any managed rule affected by this change will be updated. You should not experience any delay in reporting evaluation results for a managed rule with configuration changes.

## What is the impact on historical data? Would it still display details about indirect relationships?

Indirect relationships will be available in historical `ConfigurationItems` recorded before they are deprecated, but will not be available in `ConfigurationItems` recorded after deprecation.

## Is there a change in the output generated by `GetResourceConfigHistory` API?

The models used in the `GetResourceConfigHistory` API are not changed and there is no change to the data returned for `ConfigurationItems` recorded prior to deprecation. `ConfigurationItems` recorded after deprecation no longer include the indirect relationships in the **Relationships** field.

## Is there any change in the resource schema of a Configuration Item?

There is no change to the schema of the data in the **configuration** field in the Configuration Item. The only change is that the **relationships** field in the Configuration Item will no longer include the specified indirect relationships.

## Are there other alternatives to retrieve indirect relationships?

With the launch of Advanced queries, you can run Structured Query Language (SQL) queries. For example, if you want to retrieve the list of EC2 instances related to a security group, use the following query:

AWS Config Developer Guide  
Are there other alternatives to  
retrieve indirect relationships?

---

```
SELECT
  resourceId,
  resourceType
WHERE
  resourceType = 'AWS::EC2::Instance'
AND
  relationships.resourceId = 'sg-234213'
```

Sample relationships queries are available here: [Example Queries](#)

# Document History

The following table describes the important changes to the documentation for AWS Config. For notification about updates to this documentation, you can subscribe to an RSS feed.

- **API version:** 2014-11-12
- **Latest documentation update:** April 15, 2021

update-history-change	update-history-description	update-history-date
<a href="#">AWS Config updates managed rules (p. 3327)</a>	<p>With this release, AWS Config supports the following managed rules:</p> <ul style="list-style-type: none"> <li>• <a href="#">aurora-mysql-backtracking-enabled</a></li> <li>• <a href="#">ec2-instance-profile-attached</a></li> <li>• <a href="#">ecs-task-definition-user-for-host-mode-check</a></li> <li>• <a href="#">no-unrestricted-route-to-igw</a></li> <li>• <a href="#">rds-automatic-minor-version-upgrade-enabled</a></li> <li>• <a href="#">redshift-enhanced-vpc-routing-enabled</a></li> </ul>	April 15, 2021
<a href="#">Security IAM update (p. 3327)</a>	<p>The <code>AWSConfigServiceRolePolicy</code> policy and <code>AWS_ConfigRole</code> policy now grant permission to view information about AWS Systems Manager (formerly known as SSM) specified documents. These policies also now support additional AWS resource types for AWS Backup, Amazon Elastic File System, Amazon ElastiCache, Amazon Simple Storage Service, Amazon Elastic Compute Cloud, Amazon Kinesis, Amazon SageMaker, AWS Database Migration Service, and Amazon Route 53. These permission changes allow AWS Config to invoke the read-only APIs required to support these resource types. For more information, see <a href="#">AWS managed policies for AWS Config</a>.</p>	April 14, 2021
<a href="#">Conformance Pack Compliance as Configuration Items (CIs) (p. 3327)</a>	<p>With this release, AWS Config supports conformance pack compliance as configuration</p>	March 30, 2021

items. This enables you to view a timeline of changes to the compliance state of your conformance packs, aggregate conformance packs compliance across multiple accounts and regions, and use advanced queries to check the compliance of your conformance packs.

The following API's are updated:

- [DescribeAggregateComplianceByConformancePacks](#)
- [GetAggregateConformancePackComplianceSummary](#)

The following pages in the developer guide are updated:

- [Viewing Compliance Data in the Conformance Packs Dashboard](#)
- [Viewing Compliance History Timeline for Conformance Packs](#)
- [Viewing Compliance Data in the Aggregator Dashboard](#)
- [Querying the Current Configuration State of AWS Resources](#)
- [Supported Resource Types](#)

#### Pagination update (p. 3327)

With this release, AWS Config advanced queries feature now supports pagination for queries that contain aggregate functions, such as COUNT and SUM. You can now use advanced queries to get complete results for your aggregate queries through pagination, which were previously limited to 500 rows. For more information, see [Querying the Current Configuration State of AWS Resources](#)

March 26, 2021

#### Region support (p. 3327)

With this release, AWS Config and AWS Config Rules is now supported in Asia Pacific (Osaka) Region.

March 4, 2021

<a href="#">AWS Config supports new resources types (p. 3327)</a>	With this release, you can use AWS Config to record configuration changes to Amazon Elastic Container Registry, Amazon Elastic Container Service, and Amazon Elastic Kubernetes Service resource types. For more information, see <a href="#">Supported Resource Types</a> .	February 25, 2021
<a href="#">KMS encryption support (p. 3327)</a>	<p>With this release, AWS Config allows you to use KMS-based encryption on objects delivered by AWS Config for S3 bucket delivery.</p> <p>The following API's are updated:</p> <ul style="list-style-type: none"><li>• <a href="#">DeliveryChannel</a></li><li>• <a href="#">PutDeliveryChannel</a></li></ul> <p>The following pages in the developer guide are updated:</p> <ul style="list-style-type: none"><li>• <a href="#">Permissions for the KMS Key</a></li><li>• <a href="#">Permissions for the IAM Role Assigned to AWS Config</a></li></ul>	February 16, 2021
<a href="#">AWS Config updates managed rules (p. 3327)</a>	<p>With this release, AWS Config supports the following managed rules:</p> <ul style="list-style-type: none"><li>• <a href="#">secretsmanager-secret-periodic-rotation</a></li><li>• <a href="#">secretsmanager-secret-unused</a></li><li>• <a href="#">secretsmanager-using-cmk</a></li></ul>	February 16, 2021
<a href="#">Saved Query Region support (p. 3327)</a>	With this release, saved query is now supported in AWS GovCloud (US-East) and AWS GovCloud (US-West) Regions.	February 15, 2021
<a href="#">Multi-account multi-region data aggregation Region support (p. 3327)</a>	With this release, multi-account multi-region data aggregation is now supported in Africa (Cape Town) and Europe (Milan) Regions. For more information, see <a href="#">Multi-Account Multi-Region Data Aggregation</a> .	February 15, 2021

<a href="#">Advanced queries Region support (p. 3327)</a>	<p>With this release, advanced queries is now supported in Africa (Cape Town) and Europe (Milan) Regions. For more information, see <a href="#">Querying the Current Configuration State of AWS Resources</a>.</p>	<p>February 15, 2021</p>
<a href="#">AWS Config documentation history notification available through RSS feed (p. 3327)</a>	<p>You can now receive notification about updates to the AWS Config documentation by subscribing to an RSS feed.</p>	<p>January 1, 2021</p>

## Earlier Updates

The following table describes the documentation release history of AWS Config prior to Dec 31, 2020.

Change	Description	Release Date
<p>Saved Query support</p>	<p>With this release, AWS Config allows you to save your queries. After you save the query, you can search it, copy it to the query editor, edit it, or delete it. For more information about how to save a query, see the <a href="#">Query Using the SQL Query Editor (Console) (p. 70)</a> and <a href="#">Query Using the SQL Query Editor (AWS CLI) (p. 71)</a>.</p> <p>For more information about APIs, see the <i>AWS Config API Reference</i>:</p> <ul style="list-style-type: none"> <li>• <a href="#">PutStoredQuery</a></li> <li>• <a href="#">GetStoredQuery</a></li> <li>• <a href="#">ListStoredQueries</a></li> <li>• <a href="#">DeleteStoredQuery</a></li> </ul> <p>Also see <a href="#">Service Limits (p. 23)</a>.</p>	<p>December 21, 2020</p>
<p>Process checks support</p>	<p>With this release, AWS Config supports process checks that is a type of AWS Config rule that allows you to track your external and internal tasks that require verification as part of the conformance packs. With process checks, you can list the compliance of requirements and actions at a single location.</p> <p>For more information about process checks, see the <a href="#">AWS Config Process Checks Within a Conformance Pack (p. 222)</a> topic and the <a href="#">PutExternalEvaluation</a> API.</p>	<p>December 17, 2020</p>

Change	Description	Release Date
<p>AWS Config updates managed rules</p>	<p>With this release, AWS Config supports the following managed rules:</p> <ul style="list-style-type: none"> <li>• <a href="#">api-gw-ssl-enabled</a> (p. 111)</li> <li>• <a href="#">api-gw-xray-enabled</a> (p. 111)</li> <li>• <a href="#">beanstalk-enhanced-health-reporting-enabled</a> (p. 113)</li> <li>• <a href="#">cloudfront-accesslogs-enabled</a> (p. 115)</li> <li>• <a href="#">cloudfront-associated-with-waf</a> (p. 115)</li> <li>• <a href="#">cloudfront-custom-ssl-certificate</a> (p. 116)</li> <li>• <a href="#">elastic-beanstalk-managed-updates-enabled</a> (p. 142)</li> <li>• <a href="#">rds-cluster-iam-authentication-enabled</a> (p. 165)</li> <li>• <a href="#">redshift-cluster-kms-enabled</a> (p. 170)</li> <li>• <a href="#">s3-bucket-level-public-access-prohibited</a> (p. 177)</li> <li>• <a href="#">subnet-auto-assign-public-ip-disabled</a> (p. 188)</li> <li>• <a href="#">vpc-network-acl-unused-check</a> (p. 189)</li> </ul>	<p>December 17, 2020</p>
<p>AWS Config supports AWS Network Firewall</p>	<p>With this release, you can use AWS Config to record configuration changes to your AWS Network Firewall FirewallPolicy, RuleGroup, and Firewall resource types. For more information, see <a href="#">Supported Resource Types</a> (p. 9).</p>	<p>December 4, 2020</p>
<p>Documentation update</p>	<p>AWS Config added support for organization-wide resource data aggregation in a delegated administrator account. You can now use a delegated administrator account to aggregate resource configuration and compliance data from all member accounts of an organization in AWS Organizations.</p> <p>For more information, see <a href="#">PutConfigurationAggregator</a>, <a href="#">Setting Up an Aggregator Using the Console</a> (p. 3266) and <a href="#">Register a Delegated Administrator</a> (p. 3270).</p>	<p>December 4, 2020</p>

Change	Description	Release Date
<p>AWS Config supports new conformance packs</p>	<ul style="list-style-type: none"> <li>• <a href="#">Operational Best Practices for CMMC Level 3</a> (p. 914)</li> <li>• <a href="#">Operational Best Practices for CMMC Level 4</a> (p. 1049)</li> <li>• <a href="#">Operational Best Practices for CMMC Level 5</a> (p. 1195)</li> <li>• <a href="#">Operational Best Practices for Esquema Nacional de Seguridad (ENS) Low</a> (p. 1362)</li> <li>• <a href="#">Operational Best Practices for Esquema Nacional de Seguridad (ENS) Medium</a> (p. 1436)</li> <li>• <a href="#">Operational Best Practices for NCSC Cyber Assessment Framework</a> (p. 2608)</li> <li>• <a href="#">Operational Best Practices for RBI Cyber Security Framework for UCBs</a> (p. 3177)</li> </ul>	<p>October 30, 2020</p>
<p>AWS Config supports new conformance packs</p>	<ul style="list-style-type: none"> <li>• <a href="#">Operational Best Practices for ACSC Essential 8</a> (p. 372)</li> <li>• <a href="#">Operational Best Practices for ACSC ISM</a> (p. 398)</li> <li>• <a href="#">Operational Best Practices for AI and ML</a> (p. 419)</li> <li>• <a href="#">Operational Best Practices for Asset Management</a> (p. 513)</li> <li>• <a href="#">Operational Best Practices for BCP and DR</a> (p. 566)</li> <li>• <a href="#">Operational Best Practices for EC2</a> (p. 1361)</li> <li>• <a href="#">Operational Best Practices for K-ISMS</a> (p. 2054)</li> <li>• <a href="#">Operational Best Practices for Load Balancing</a> (p. 2100)</li> <li>• <a href="#">Operational Best Practices for Logging</a> (p. 2100)</li> <li>• <a href="#">Operational Best Practices for Monitoring</a> (p. 2260)</li> <li>• <a href="#">Operational Best Practices for Serverless</a> (p. 3251)</li> </ul>	<p>October 22, 2020</p>

Change	Description	Release Date
<p>AWS Config supports new conformance packs</p>	<ul style="list-style-type: none"> <li>• <a href="#">Operational Best Practices for APRA CPG 234</a> (p. 420)</li> <li>• <a href="#">Operational Best Practices for FedRAMP(Low)</a> (p. 1674)</li> <li>• <a href="#">Operational Best Practices for MAS Notice 655</a> (p. 2101)</li> <li>• <a href="#">Operational Best Practices for NBC TRMG</a> (p. 2260)</li> <li>• <a href="#">Operational Best Practices for NCSC Cloud Security Principles</a> (p. 2586)</li> <li>• <a href="#">Operational Best Practices for RBI MD-ITF</a> (p. 3194)</li> </ul>	<p>October 15, 2020</p>
<p>AWS Config supports new conformance packs</p>	<ul style="list-style-type: none"> <li>• <a href="#">Operational Best Practices for ABS CCIG 2.0 Material Workloads</a> (p. 227)</li> <li>• <a href="#">Operational Best Practices for ABS CCIG 2.0 Standard Workloads</a> (p. 313)</li> <li>• <a href="#">Operational Best Practices for BNM RMIT</a> (p. 567)</li> <li>• <a href="#">Operational Best Practices for Data Resiliency</a> (p. 1360)</li> <li>• <a href="#">Operational Best Practices for Data Lakes and Analytics Services</a> (p. 1361)</li> <li>• <a href="#">Operational Best Practices for Encryption and Key Management</a> (p. 1361)</li> <li>• <a href="#">Operational Best Practices for FDA Title 21 CFR Part 11</a> (p. 1528)</li> <li>• <a href="#">Operational Best Practices for Publicly Accessible Resources</a> (p. 3176)</li> <li>• <a href="#">Operational Best Practices for MAS TRMG June 2013</a> (p. 2116)</li> <li>• <a href="#">Operational Best Practices for NERC CIP</a> (p. 2522)</li> <li>• <a href="#">Operational Best Practices for NYDFS 23</a> (p. 3054)</li> </ul>	<p>October 8, 2020</p>

Change	Description	Release Date
AWS Config supports new conformance packs	<ul style="list-style-type: none"> <li>• <a href="#">Operational Best Practices for AWS Well-Architected Framework Reliability Pillar</a> (p. 514)</li> <li>• <a href="#">Operational Best Practices for AWS Well-Architected Framework Security Pillar</a> (p. 520)</li> <li>• <a href="#">Operational Best Practices for CMMC Level 1</a> (p. 758)</li> <li>• <a href="#">Operational Best Practices for CMMC Level 2</a> (p. 804)</li> <li>• <a href="#">Operational Best Practices for Compute Services</a> (p. 1360)</li> <li>• <a href="#">Operational Best Practices for Databases Services</a> (p. 1361)</li> <li>• <a href="#">Operational Best Practices for Management and Governance Services</a> (p. 2100)</li> <li>• <a href="#">Operational Best Practices for Networking and Content Delivery Services</a> (p. 2658)</li> <li>• <a href="#">Operational Best Practices for Security, Identity, and Compliance Services</a> (p. 3251)</li> <li>• <a href="#">Operational Best Practices for Storage Services</a> (p. 3251)</li> </ul>	September 30, 2020
AWS Config supports new conformance packs	<ul style="list-style-type: none"> <li>• <a href="#">Operational Best Practices for FedRAMP(Moderate)</a> (p. 1705)</li> <li>• <a href="#">Operational Best Practices for FFIEC</a> (p. 1865)</li> <li>• <a href="#">Operational Best Practices for HIPAA Security</a> (p. 1954)</li> <li>• <a href="#">Operational Best Practices for NIST 800-53 rev 4</a> (p. 2658)</li> <li>• <a href="#">Operational Best Practices for NIST 800 171</a> (p. 2821)</li> </ul>	September 28, 2020
Documentation update	<p>The following conformance pack topics are updated.</p> <ul style="list-style-type: none"> <li>• <a href="#">Prerequisites</a> (p. 219)</li> <li>• <a href="#">Deploying a Conformance Pack Using the AWS Config Console</a> (p. 3252)</li> <li>• <a href="#">Managing Conformance Packs Across all Accounts in Your Organization</a> (p. 3257)</li> </ul>	September 28, 2020

Change	Description	Release Date
AWS Config updates managed rules	<p>With this release, AWS Config supports the following managed rules:</p> <ul style="list-style-type: none"> <li>• <a href="#">iam-customer-policy-blocked-kms-actions</a> (p. 153)</li> <li>• <a href="#">iam-inline-policy-blocked-kms-actions</a> (p. 153)</li> </ul>	September 17, 2020
AWS Config supports AWS WAFv2	<p>With this release, you can use AWS Config to record configuration changes to your AWS WAFv2 WebACL, IPSet, RegexPatternSet, RuleGroup, and ManagedRuleSet resource types. For more information, see <a href="#">Supported Resource Types</a> (p. 9).</p>	September 1, 2020
Documentation update	<p>A note has been added to <a href="#">Granting Custom Permissions for AWS Config Users</a> (p. 3281) about creating custom permissions that grant full access.</p> <p>The documentation has been updated for the following rules:</p> <ul style="list-style-type: none"> <li>• <a href="#">s3-bucket-server-side-encryption-enabled</a> (p. 181)</li> <li>• <a href="#">ec2-instance-detailed-monitoring-enabled</a> (p. 132)</li> <li>• <a href="#">ec2-managedinstance-platform-check</a> (p. 136)</li> </ul>	August 24, 2020
Documentation update	<p><a href="#">Operational Best Practices for PCI DSS 3.2.1</a> (p. 3122) and <a href="#">Operational Best Practices for NIST CSF</a> (p. 2954) templates are updated.</p>	August 14, 2020
Documentation update	<p>Example relationship queries are added. For more information, see <a href="#">Example Relationship Queries</a> (p. 78).</p>	July 30, 2020
Documentation update	<p>The following API's are updated:</p> <ul style="list-style-type: none"> <li>• <a href="#">ConfigurationAggregator</a></li> <li>• <a href="#">RemediationConfiguration</a></li> <li>• <a href="#">DescribeOrganizationConfigRules</a></li> <li>• <a href="#">GetOrganizationConfigRuleDetailedStatus</a></li> <li>• <a href="#">DescribeOrganizationConfigRuleStatuses</a></li> <li>• <a href="#">DescribeOrganizationConformancePacks</a></li> <li>• <a href="#">DescribeOrganizationConformancePackStatuses</a></li> <li>• <a href="#">GetOrganizationConformancePackDetailedStatus</a></li> </ul>	July 23, 2020

Change	Description	Release Date
AWS Config supports AWS Systems Manager resource type	With this release, you can use AWS Config to record configuration changes to the AWS Systems Manager file data resource type. For more information, see <a href="#">Supported Resource Types (p. 9)</a> .	July 9, 2020
Documentation update	<a href="#">Operational Best Practices for AWS Identity And Access Management (p. 513)</a> and <a href="#">Operational Best Practices for PCI DSS 3.2.1 (p. 3122)</a> templates are updated.	July 9, 2020

Change	Description	Release Date
<p>AWS Config updates managed rules</p>	<p>With this release, AWS Config supports the following managed rules:</p> <ul style="list-style-type: none"> <li>• <a href="#">account-part-of-organizations</a> (p. 108)</li> <li>• <a href="#">alb-http-drop-invalid-header-enabled</a> (p. 109)</li> <li>• <a href="#">alb-waf-enabled</a> (p. 109)</li> <li>• <a href="#">cloudfront-default-root-object-configured</a> (p. 116)</li> <li>• <a href="#">cloudfront-origin-access-identity-enabled</a> (p. 116)</li> <li>• <a href="#">cloudfront-origin-failover-enabled</a> (p. 117)</li> <li>• <a href="#">cloudfront-sni-enabled</a> (p. 117)</li> <li>• <a href="#">cloudtrail-security-trail-enabled</a> (p. 118)</li> <li>• <a href="#">cw-loggroup-retention-period-check</a> (p. 125)</li> <li>• <a href="#">dax-encryption-enabled</a> (p. 125)</li> <li>• <a href="#">dynamodb-in-backup-plan</a> (p. 128)</li> <li>• <a href="#">ebs-in-backup-plan</a> (p. 130)</li> <li>• <a href="#">ec2-imdsv2-check</a> (p. 132)</li> <li>• <a href="#">efs-in-backup-plan</a> (p. 139)</li> <li>• <a href="#">eks-endpoint-no-public-access</a> (p. 139)</li> <li>• <a href="#">eks-secrets-encrypted</a> (p. 140)</li> <li>• <a href="#">elasticsearch-node-to-node-encryption-check</a> (p. 142)</li> <li>• <a href="#">elb-cross-zone-load-balancing-enabled</a> (p. 143)</li> <li>• <a href="#">elb-tls-https-listeners-only</a> (p. 145)</li> <li>• <a href="#">iam-no-inline-policy-check</a> (p. 154)</li> <li>• <a href="#">rds-cluster-deletion-protection-enabled</a> (p. 164)</li> <li>• <a href="#">rds-in-backup-plan</a> (p. 167)</li> <li>• <a href="#">rds-instance-deletion-protection-enabled</a> (p. 166)</li> <li>• <a href="#">rds-instance-iam-authentication-enabled</a> (p. 166)</li> <li>• <a href="#">rds-logging-enabled</a> (p. 167)</li> <li>• <a href="#">redshift-backup-enabled</a> (p. 169)</li> <li>• <a href="#">waf-classic-logging-enabled</a> (p. 190)</li> <li>• <a href="#">wafv2-logging-enabled</a> (p. 190)</li> </ul> <p>For more information, see <a href="#">List of AWS Config Managed Rules</a> (p. 103).</p>	<p>July 9, 2020</p>

Change	Description	Release Date
Multi-account multi-region data aggregation Region support	With this release, multi-account multi-region data aggregation is now supported in Asia Pacific (Hong Kong) and Middle East (Bahrain) Regions. For more information, see <a href="#">Multi-Account Multi-Region Data Aggregation (p. 3262)</a> and <a href="#">Troubleshooting for Multi-Account Multi-Region Data Aggregation (p. 3277)</a> .	July 1, 2020
Advanced queries Region support	With this release, advanced queries is now supported in Asia Pacific (Hong Kong) and Middle East (Bahrain) Regions. For more information, see <a href="#">Querying the Current Configuration State of AWS Resources (p. 66)</a> .	July 1, 2020
Documentation update	The documentation has been updated for the following rules: <ul style="list-style-type: none"> <li>• <a href="#">ec2-managedinstance-association-compliance-status-check (p. 135)</a></li> <li>• <a href="#">iam-policy-no-statements-with-admin-access (p. 156)</a></li> <li>• <a href="#">required-tags (p. 172)</a></li> <li>• <a href="#">restricted-common-ports (p. 174)</a></li> <li>• <a href="#">rds-snapshots-public-prohibited (p. 168)</a></li> <li>• <a href="#">s3-bucket-policy-grantee-check (p. 178)</a></li> </ul>	June 30, 2020
Documentation update	The documentation has been updated with information about security for AWS Config. See <a href="#">Security in AWS Config (p. 3278)</a> .	June 24, 2020
Documentation update	AWS Control Tower Detective Guardrails Conformance Pack template is updated. For more information, see <a href="#">AWS Control Tower Detective Guardrails Conformance Pack (p. 227)</a> .	June 4, 2020
AWS Config supports a new conformance pack	With this release, AWS Config supports Operational Best Practices for NIST CSF conformance pack. For more information, see <a href="#">Operational Best Practices for NIST CSF (p. 2954)</a> .	May 29, 2020

Change	Description	Release Date
AWS Config updates managed rules	<p>With this release, AWS Config supports the following managed rules:</p> <ul style="list-style-type: none"> <li>• <a href="#">dynamodb-pitr-enabled</a> (p. 129)</li> <li>• <a href="#">dynamodb-table-encrypted-kms</a> (p. 129)</li> <li>• <a href="#">ec2-ebs-encryption-by-default</a> (p. 131)</li> <li>• <a href="#">rds-snapshot-encrypted</a> (p. 168)</li> <li>• <a href="#">redshift-require-tls-ssl</a> (p. 172)</li> <li>• <a href="#">s3-bucket-default-lock-enabled</a> (p. 177)</li> <li>• <a href="#">s3-default-encryption-kms</a> (p. 182)</li> <li>• <a href="#">securityhub-enabled</a> (p. 186)</li> <li>• <a href="#">sns-encrypted-kms</a> (p. 187)</li> </ul> <p>For more information, see <a href="#">List of AWS Config Managed Rules</a> (p. 103).</p>	May 28, 2020
Delegated administrator support	<p>With this release, you can deploy AWS Config rules and conformance packs from any delegated member account in your organization, in addition to the management account.</p> <p>For more information about APIs, see the <i>AWS Config API Reference</i>:</p> <ul style="list-style-type: none"> <li>• <a href="#">PutOrganizationConfigRule</a></li> <li>• <a href="#">PutOrganizationConformancePack</a></li> <li>• <a href="#">DescribeOrganizationConfigRules</a></li> <li>• <a href="#">GetOrganizationConfigRuleDetailedStatus</a></li> <li>• <a href="#">DescribeOrganizationConfigRuleStatuses</a></li> <li>• <a href="#">DeleteOrganizationConfigRule</a></li> <li>• <a href="#">DeleteOrganizationConformancePack</a></li> <li>• <a href="#">DescribeOrganizationConformancePacks</a></li> <li>• <a href="#">DescribeOrganizationConformancePackStatuses</a></li> <li>• <a href="#">GetOrganizationConformancePackDetailedStatus</a></li> </ul> <p>For more information, see <a href="#">Service Limits</a> (p. 23).</p>	May 27, 2020
AWS Config rules Region support	<p>With this release, few AWS Config rules are supported in Africa (Cape Town) and Europe (Milan) regions. For a detailed list of rules and the regions they are supported in, see <a href="#">List of AWS Config Managed Rules</a> (p. 103).</p>	April 28, 2020

Change	Description	Release Date
AWS Config supports new conformance packs	<p>With this release, AWS Config supports two conformance packs.</p> <ul style="list-style-type: none"> <li>• AWS Control Tower Detective Guardrails Conformance Pack</li> <li>• Operational Best Practices for CIS</li> </ul> <p>For more information, see <a href="#">Conformance Pack Sample Templates (p. 225)</a>.</p>	April 22, 2020
AWS Config supports AWS Secrets Manager	<p>With this release, you can use AWS Config to record configuration changes to your Secrets Manager secret. For more information, see <a href="#">Supported Resource Types (p. 9)</a>.</p>	April 20, 2020
AWS Config updates managed rules	<p>With this release, AWS Config supports the following managed rules:</p> <ul style="list-style-type: none"> <li>• <a href="#">secretsmanager-rotation-enabled-check (p. 183)</a></li> <li>• <a href="#">secretsmanager-scheduled-rotation-success-check (p. 184)</a></li> </ul> <p>For more information, see <a href="#">List of AWS Config Managed Rules (p. 103)</a>.</p>	April 16, 2020
Conformance pack Region support	<p>With this release, conformance packs are now supported in Asia Pacific (Hong Kong) and Middle East (Bahrain). For more information, see <a href="#">Conformance Packs (p. 219)</a>.</p>	April 8, 2020
Documentation update	<p>AWS Config limits are available in this developer guide. For more information, see <a href="#">Service Limits (p. 23)</a>.</p>	April 8, 2020
Documentation update	<p>Third-party resources that are managed (i.e. created/updated/deleted) through AWS CloudFormation registry are automatically tracked in AWS Config as configuration items. For more information, see <a href="#">Record Configurations for Third-Party Resources (p. 38)</a>.</p>	March 30, 2020
Documentation update	<p>The AWS Config Managed Rules are updated to include AWS Region information. For more information, see <a href="#">List of AWS Config Managed Rules (p. 103)</a>.</p>	March 27, 2020

Change	Description	Release Date
AWS Config supports Amazon SNS resource type	With this release, you can use AWS Config to record configuration changes to your Amazon SNS topic. For more information, see <a href="#">Supported Resource Types (p. 9)</a> .	March 6, 2020
Multi-account multi-region data aggregation Region support	With this release, multi-account multi-region data aggregation is now supported in Europe (Stockholm) Region. For more information, see <a href="#">Multi-Account Multi-Region Data Aggregation (p. 3262)</a> .	March 5, 2020
Advanced queries Region support	With this release, advanced queries is now supported in Europe (Stockholm) Region. For more information, see <a href="#">Querying the Current Configuration State of AWS Resources (p. 66)</a> .	March 5, 2020
AWS Config allows you to run advanced queries with configuration aggregators	<p>With this release, AWS Config adds support to run advanced queries based on resource configuration properties with configuration aggregators, enabling you to run the same queries across multiple accounts and Regions. For more information, see <a href="#">Querying the Current Configuration State of AWS Resources (p. 66)</a>.</p> <p>With this release, AWS Config adds <code>SelectAggregateResourceConfig</code> API. For more information, see <a href="#">SelectAggregateResourceConfig</a> in the <i>AWS Config API Reference</i>:</p>	February 28, 2020
AWS Config supports Amazon SQS resource type	<p>With this release, you can use AWS Config to record configuration changes to your Amazon SQS queue.</p> <p>For more information, see <a href="#">Supported Resource Types (p. 9)</a>.</p>	February 13, 2020

Change	Description	Release Date
<p>AWS CloudFormation support for Conformance packs</p>	<p>With this release, AWS CloudFormation support for the following resources was added:  <code>AWS::Config::ConformancePack</code>  and  <code>OrganizationConformancePack</code>.</p> <ul style="list-style-type: none"> <li>• <a href="#">AWS::Config::ConformancePack</a></li> </ul> <p>Use the <code>AWS::Config::ConformancePack</code> resource to create a Conformance Pack that is a collection of AWS Config rules that can be easily deployed in an account and a Region and across AWS Organization.</p> <ul style="list-style-type: none"> <li>• <a href="#">AWS::Config::OrganizationConformancePack</a></li> </ul> <p>Use the <code>AWS::Config::OrganizationConformancePack</code> resource to create an Organization Conformance Pack that has information about conformance packs that AWS Config creates in the member accounts.</p>	<p>February 13, 2020</p>
<p>AWS Config updates managed rules</p>	<p>With this release, AWS Config supports the following managed rules:</p> <ul style="list-style-type: none"> <li>• <a href="#">api-gw-execution-logging-enabled</a> (p. 111)</li> <li>• <a href="#">ec2-stopped-instance</a> (p. 137)</li> <li>• <a href="#">elasticache-redis-cluster-automatic-backup-check</a> (p. 140)</li> <li>• <a href="#">emr-master-no-public-ip</a> (p. 146)</li> <li>• <a href="#">guardduty-non-archived-findings</a> (p. 152)</li> <li>• <a href="#">rds-enhanced-monitoring-enabled</a> (p. 165)</li> <li>• <a href="#">s3-account-level-public-access-blocks</a> (p. 175)</li> <li>• <a href="#">sagemaker-endpoint-configuration-kms-key-configured</a> (p. 182)</li> <li>• <a href="#">service-vpc-endpoint-enabled</a> (p. 186)</li> </ul> <p>For more information, see <a href="#">List of AWS Config Managed Rules</a> (p. 103).</p>	<p>December 20, 2019</p>

Change	Description	Release Date
Record configurations for custom resource types	<p>With this release, AWS Config introduces support to record configurations for custom resource types. You can publish the configuration data of third-party resources into AWS Config and view and monitor the resource inventory and configuration history using AWS Config console and APIs. For more information, see <a href="#">Record Configurations for Third-Party Resources (p. 38)</a>.</p> <p>For more information about APIs, see the <i>AWS Config API Reference</i>:</p> <ul style="list-style-type: none"> <li>• <a href="#">DeleteResourceConfig</a></li> <li>• <a href="#">PutResourceConfig</a></li> </ul>	November 20, 2019
Conformance packs	<p>With this release, AWS Config introduces conformance packs. Conformance packs enable you to package a collection of AWS Config rules and remediation actions that can then be deployed together as a single entity across an entire AWS Organization. For more information, see <a href="#">Conformance Packs (p. 219)</a>.</p> <p>For more information about APIs, see the <i>AWS Config API Reference</i>:</p> <ul style="list-style-type: none"> <li>• <a href="#">DeleteOrganizationConformancePack</a></li> <li>• <a href="#">DeleteOrganizationConformancePack</a></li> <li>• <a href="#">DescribeConformancePacks</a></li> <li>• <a href="#">DescribeConformancePacks</a></li> <li>• <a href="#">DescribeConformancePackStatus</a></li> <li>• <a href="#">DescribeOrganizationConformancePacks</a></li> <li>• <a href="#">DescribeOrganizationConformancePackStatuses</a></li> <li>• <a href="#">GetConformancePackComplianceDetails</a></li> <li>• <a href="#">GetConformancePackComplianceSummary</a></li> <li>• <a href="#">GetOrganizationConformancePackDetailedStatus</a>,</li> <li>• <a href="#">PutConformancePack</a></li> <li>• <a href="#">PutOrganizationConformancePack</a></li> </ul>	November 19, 2019
AWS Config supports Amazon Elasticsearch Service and AWS Key Management Service resource types	<p>With this release, you can use AWS Config to record configuration changes to your Amazon Elasticsearch Service domain and AWS Key Management Service key.</p> <p>For more information, see <a href="#">Supported Resource Types (p. 9)</a>.</p>	November 11, 2019

Change	Description	Release Date
<p>AWS Config updates managed rules</p>	<p>With this release, AWS Config supports the following managed rules:</p> <ul style="list-style-type: none"> <li>• <a href="#">dms-replication-not-public</a> (p. 127)</li> <li>• <a href="#">emr-kerberos-enabled</a> (p. 145)</li> <li>• <a href="#">fms-security-groups-audit-policy-check</a> (p. 147)</li> <li>• <a href="#">fms-security-groups-content-check</a> (p. 148)</li> <li>• <a href="#">fms-security-groups-resource-association-check</a> (p. 148)</li> <li>• <a href="#">internet-gateway-authorized-vpc-only</a> (p. 160)</li> <li>• <a href="#">kms-cmk-not-scheduled-for-deletion</a> (p. 160)</li> <li>• <a href="#">sagemaker-notebook-no-direct-internet-access</a> (p. 183)</li> <li>• <a href="#">sagemaker-notebook-instance-kms-key-configured</a> (p. 183)</li> <li>• <a href="#">shield-drt-access</a> (p. 187)</li> </ul> <p>For more information, see <a href="#">List of AWS Config Managed Rules</a> (p. 103).</p>	<p>October 10, 2019</p>
<p>AWS Config supports Amazon RDS resource type</p>	<p>With this release, you can use AWS Config to record configuration changes to your Amazon Relational Database Service (Amazon RDS) DBCluster and DBClusterSnapshot.</p> <p>For more information, see <a href="#">Supported Resource Types</a> (p. 9).</p>	<p>September 17, 2019</p>
<p>AWS Config supports Amazon QLDB resource type</p>	<p>With this release, you can use AWS Config to record configuration changes to Amazon Quantum Ledger Database (QLDB) ledger resource type.</p> <p>For more information, see <a href="#">Supported Resource Types</a> (p. 9).</p>	<p>September 10, 2019</p>

Change	Description	Release Date
<p>AWS Config allows you to apply auto remediation on noncompliant resources as evaluated by AWS Config Rules</p>	<p>With this release, AWS Config introduces support to apply auto remediation using AWS Systems Manager automation documents on noncompliant resources as evaluated by AWS Config Rules. For more information, see <a href="#">Remediating Noncompliant AWS Resources by AWS Config Rules</a> (p. 213).</p> <p>With this release, AWS Config adds the following new APIs. For more information, see the <i>AWS Config API Reference</i> :</p> <ul style="list-style-type: none"> <li>• <a href="#">PutRemediationExceptions</a></li> <li>• <a href="#">DescribeRemediationExceptions</a></li> <li>• <a href="#">DeleteRemediationExceptions</a></li> </ul>	<p>September 5, 2019</p>
<p>AWS Config updates managed rules</p>	<p>With this release, AWS Config supports the following managed rules:</p> <ul style="list-style-type: none"> <li>• <a href="#">alb-http-to-https-redirect-check</a> (p. 109)</li> <li>• <a href="#">api-gw-cache-enabled-and-encrypted</a> (p. 110)</li> <li>• <a href="#">api-gw-endpoint-type-check</a> (p. 110)</li> <li>• <a href="#">cloudtrail-s3-dataevents-enabled</a> (p. 118)</li> <li>• <a href="#">cloudwatch-log-group-encrypted</a> (p. 121)</li> <li>• <a href="#">ebs-snapshot-public-restorable-check</a> (p. 131)</li> <li>• <a href="#">elb-deletion-protection-enabled</a> (p. 144)</li> <li>• <a href="#">lambda-concurrency-check</a> (p. 161)</li> <li>• <a href="#">lambda-dlq-check</a> (p. 161)</li> <li>• <a href="#">lambda-inside-vpc</a> (p. 162)</li> <li>• <a href="#">shield-advanced-enabled-autorenew</a> (p. 186)</li> <li>• <a href="#">vpc-vpn-2-tunnels-up</a> (p. 189)</li> </ul> <p>For more information, see <a href="#">List of AWS Config Managed Rules</a> (p. 103).</p>	<p>August 22, 2019</p>

Change	Description	Release Date
<p>AWS Config updates managed rules</p>	<p>With this release, AWS Config updates the following managed rules:</p> <ul style="list-style-type: none"> <li>• <a href="#">cloudfront-viewer-policy-https</a> (p. 117)</li> <li>• <a href="#">ec2-instance-no-public-ip</a> (p. 133)</li> <li>• <a href="#">ec2-security-group-attached-to-eni</a> (p. 137)</li> <li>• <a href="#">efs-encrypted-check</a> (p. 138)</li> <li>• <a href="#">elasticsearch-encrypted-at-rest</a> (p. 141)</li> <li>• <a href="#">elasticsearch-in-vpc-only</a> (p. 141)</li> <li>• <a href="#">redshift-cluster-public-access-check</a> (p. 171)</li> <li>• <a href="#">vpc-sg-open-only-to-authorized-ports</a> (p. 189)</li> </ul> <p>For more information, see <a href="#">List of AWS Config Managed Rules</a> (p. 103).</p>	<p>July 31, 2019</p>
<p>AWS Config supports Amazon EC2 resource types</p>	<p>With this release, you can use AWS Config to record configuration changes to the following Amazon EC2 resources; VPCEndpoint, VPCEndpointService, and VPCPeeringConnection.</p> <p>For more information, see <a href="#">Supported Resource Types</a> (p. 9).</p>	<p>July 12, 2019</p>
<p>AWS Config allows you to manage AWS Config rules across all AWS accounts within an organization</p>	<p>With this release, AWS Config introduces support for managing AWS Config rules across all AWS accounts within an organization. You can centrally create, update, and delete AWS Config rules across all accounts in your organization. For more information, see <a href="#">Enabling AWS Config Rules Across all Accounts in Your Organization</a> (p. 212).</p> <p>For more information about APIs, see the <i>AWS Config API Reference</i>:</p> <ul style="list-style-type: none"> <li>• <a href="#">PutOrganizationConfigRule</a></li> <li>• <a href="#">DescribeOrganizationConfigRules</a></li> <li>• <a href="#">GetOrganizationConfigRuleDetailedStatus</a></li> <li>• <a href="#">DescribeOrganizationConfigRuleStatuses</a></li> <li>• <a href="#">DeleteOrganizationConfigRule</a></li> </ul>	<p>July 9, 2019</p>

Change	Description	Release Date
AWS Config supports Amazon S3 and Amazon EC2 resource types	<p>With this release, you can use AWS Config to record configuration changes to the Amazon S3 AccountPublicAccessBlock resource and the following Amazon EC2 resources; NatGateway, EgressOnlyInternetGateway, and FlowLog.</p> <p>For more information, see <a href="#">Supported Resource Types (p. 9)</a>.</p>	May 17, 2019
AWS Config updates managed rules	<p>With this release, AWS Config updates the following managed rules:</p> <ul style="list-style-type: none"> <li>• <a href="#">s3-bucket-public-read-prohibited (p. 179)</a></li> <li>• <a href="#">s3-bucket-public-write-prohibited (p. 180)</a></li> </ul> <p>For more information, see <a href="#">List of AWS Config Managed Rules (p. 103)</a>.</p>	May 7, 2019
AWS Config allows you to delete a remediation action using AWS Console.	<p>With this release, AWS Config introduces support to delete a remediation action using AWS Management Console. For more information, see <a href="#">Remediating Noncompliant AWS Resources by AWS Config Rules (p. 213)</a>.</p>	April 24, 2019
AWS Config supports new managed rules	<p>This release supports a new managed rule: <a href="#">fms-shield-resource-policy-check (p. 149)</a>.</p> <p>For more information, see <a href="#">List of AWS Config Managed Rules (p. 103)</a>.</p>	April 7, 2019
AWS Config supports Amazon API Gateway resource type	<p>With this release, you can use AWS Config to record configuration changes to the following Amazon API Gateway resources; Api (WebSocket API), RestApi (REST API), Stage (WebSocket API stage), and Stage (REST API stage).</p> <p>For more information, see <a href="#">Supported Resource Types (p. 9)</a>.</p>	March 20, 2019

Change	Description	Release Date
<p>AWS Config allows you to run advanced queries</p>	<p>With this release, AWS Config adds support to run advanced queries based on resource configuration properties. For more information, see <a href="#">Querying the Current Configuration State of AWS Resources</a> (p. 66).</p> <p>With this release, AWS Config adds <code>SelectResourceConfig</code> API. For more information, see <a href="#">SelectResourceConfig</a> in the <i>AWS Config API Reference</i>:</p>	<p>March 19, 2019</p>
<p>AWS Config allows you to assign tags your AWS Config resources</p>	<p>With this release, AWS Config introduces support for tag based access control for three AWS Config resources—<code>ConfigRule</code>, <code>ConfigurationAggregator</code>, and <code>AggregationAuthorization</code>. For more information, see <a href="#">Tagging Your AWS Config Resources</a> (p. 217).</p> <p>With this release, you can add, remove or list tags from your AWS Config resources using the following APIs. For more information, see the <i>AWS Config API Reference</i>:</p> <ul style="list-style-type: none"> <li>• <a href="#">ListTagsForResource</a></li> <li>• <a href="#">TagResource</a></li> <li>• <a href="#">UntagResource</a></li> </ul>	<p>March 14, 2019</p>
<p>AWS Config allows you to apply remediation on noncompliant resources as evaluated by AWS Config Rules</p>	<p>With this release, AWS Config introduces support to apply remediation using AWS Systems Manager automation documents on noncompliant resources as evaluated by AWS Config Rules. For more information, see <a href="#">Remediating Noncompliant AWS Resources by AWS Config Rules</a> (p. 213).</p> <p>With this release, AWS Config adds the following new APIs. For more information, see the <i>AWS Config API Reference</i> :</p> <ul style="list-style-type: none"> <li>• <a href="#">DeleteRemediationConfiguration</a></li> <li>• <a href="#">DescribeRemediationConfigurations</a></li> <li>• <a href="#">DescribeRemediationExecutionStatus</a></li> <li>• <a href="#">PutRemediationConfigurations</a></li> <li>• <a href="#">StartRemediationExecution</a></li> </ul>	<p>March 12, 2019</p>

Change	Description	Release Date
<p>AWS Config supports AWS Config Rules in China (Ningxia) Region</p>	<p>This release only supports 54 AWS Config Rules in the China (Ningxia) Region. For more information, see <a href="#">List of AWS Config Managed Rules (p. 103)</a>.</p> <p>However, AWS Config does not currently support the following rules in the China (Ningxia) Region:</p> <ul style="list-style-type: none"> <li>• acm-certificate-expiration-check</li> <li>• cmk-backing-key-rotation-enabled</li> <li>• cloudformation-stack-drift-detection-check</li> <li>• cloudformation-stack-notification-check</li> <li>• cloud-trail-encryption-enabled</li> <li>• cloud-trail-log-file-validation-enabled</li> <li>• codebuild-project-envvar-awscred-check</li> <li>• codebuild-project-source-repo-url-check</li> <li>• codepipeline-deployment-count-check</li> <li>• codepipeline-region-fanout-check</li> <li>• dynamodb-table-encryption-enabled</li> <li>• elb-acm-certificate-required</li> <li>• encrypted-volumes</li> <li>• fms-webacl-resource-policy-check</li> <li>• fms-webacl-rulegroup-association-check</li> <li>• guardduty-enabled-centralized</li> <li>• lambda-function-public-access-prohibited</li> <li>• lambda-function-settings-check</li> <li>• rds-storage-encrypted</li> <li>• root-account-mfa-hardware-mfa-enabled</li> <li>• root-account-mfa-enabled</li> <li>• s3-bucket-blacklisted-actions-prohibited</li> <li>• s3-bucket-policy-grantee-check</li> <li>• s3-bucket-policy-not-more-permissive</li> <li>• s3-bucket-public-read-prohibited</li> <li>• s3-bucket-public-write-prohibited</li> <li>• s3-bucket-server-side-encryption-enabled</li> </ul>	<p>March 12, 2019</p>

Change	Description	Release Date
	<ul style="list-style-type: none"> <li>• <a href="#">s3-bucket-ssl-requests-only</a></li> </ul>	
AWS Config supports new managed rules	<p>This release supports the following new managed rules:</p> <ul style="list-style-type: none"> <li>• <a href="#">iam-user-mfa-enabled</a> (p. 158)</li> <li>• <a href="#">s3-bucket-policy-grantee-check</a> (p. 178)</li> </ul> <p>For more information, see <a href="#">List of AWS Config Managed Rules</a> (p. 103).</p>	January 21, 2019
AWS Config supports AWS Service Catalog resource type	<p>With this release, you can use AWS Config to record configuration changes to the following AWS Service Catalog resources; CloudFormation product, provisioned product, and portfolio. For more information, see <a href="#">Supported Resource Types</a> (p. 9).</p>	January 11, 2019
Service-linked AWS Config rules support	<p>With this release, AWS Config adds a new managed config rule that supports other AWS services to create AWS Config Rules in your account. For more information, see <a href="#">Service-Linked AWS Config Rules</a> (p. 3297).</p>	November 20, 2018
AWS Config allows you to aggregate configuration data of AWS resources	<p>With this release, AWS Config introduces support for aggregating the configuration data of AWS resources. For more information, see <a href="#">Viewing Compliance Data in the Aggregator Dashboard</a> (p. 3264).</p> <p>With this release, AWS Config adds the following new APIs. For more information, see the <i>AWS Config API Reference</i> :</p> <ul style="list-style-type: none"> <li>• <a href="#">BatchGetAggregateResourceConfig</a></li> <li>• <a href="#">GetAggregateDiscoveredResourceCounts</a></li> <li>• <a href="#">GetAggregateResourceConfig</a></li> <li>• <a href="#">ListAggregateDiscoveredResources</a></li> </ul>	November 19, 2018

Change	Description	Release Date
<p>AWS Config supports new managed rules</p>	<p>This release supports the following new managed rules:</p> <ul style="list-style-type: none"> <li>• <a href="#">cloudformation-stack-drift-detection-check</a> (p. 114)</li> <li>• <a href="#">codepipeline-deployment-count-check</a> (p. 124)</li> <li>• <a href="#">codepipeline-region-fanout-check</a> (p. 124)</li> </ul> <p>For more information, see <a href="#">List of AWS Config Managed Rules</a> (p. 103).</p>	<p>November 19, 2018</p>
<p>AWS Config supports new managed rules</p>	<p>This release supports the following new managed rules:</p> <ul style="list-style-type: none"> <li>• <a href="#">access-keys-rotated</a> (p. 107)</li> <li>• <a href="#">cloud-trail-cloud-watch-logs-enabled</a> (p. 121)</li> <li>• <a href="#">cloud-trail-encryption-enabled</a> (p. 122)</li> <li>• <a href="#">cloud-trail-log-file-validation-enabled</a> (p. 122)</li> <li>• <a href="#">cmk-backing-key-rotation-enabled</a> (p. 123)</li> <li>• <a href="#">iam-policy-no-statements-with-admin-access</a> (p. 156)</li> <li>• <a href="#">iam-role-managed-policy-check</a> (p. 157)</li> <li>• <a href="#">iam-root-access-key-check</a> (p. 157)</li> <li>• <a href="#">iam-user-unused-credentials-check</a> (p. 159)</li> <li>• <a href="#">mfa-enabled-for-iam-console-access</a> (p. 163)</li> <li>• <a href="#">multi-region-cloudtrail-enabled</a> (p. 163)</li> <li>• <a href="#">root-account-hardware-mfa-enabled</a> (p. 175)</li> <li>• <a href="#">vpc-flow-logs-enabled</a> (p. 188)</li> </ul> <p>For more information, see <a href="#">List of AWS Config Managed Rules</a> (p. 103).</p>	<p>November 12, 2018</p>

Change	Description	Release Date
AWS Config supports new managed rules	<p>This release supports the following new managed rules:</p> <ul style="list-style-type: none"> <li>• <a href="#">dynamodb-table-encryption-enabled</a> (p. 129)</li> <li>• <a href="#">elb-logging-enabled</a> (p. 144)</li> <li>• <a href="#">rds-instance-public-access-check</a> (p. 166)</li> <li>• <a href="#">vpc-default-security-group-closed</a> (p. 188)</li> </ul> <p>For more information, see <a href="#">List of AWS Config Managed Rules</a> (p. 103).</p>	October 24, 2018
Compliance history support	<p>With this release, AWS Config now supports storing compliance history of resources as evaluated by AWS Config Rules. For more information, see <a href="#">Viewing Compliance History Timeline for Resources</a> (p. 49).</p>	October 18, 2018
Multi-account multi-region Data Aggregation Region support	<p>With this release, multi-account multi-region Data Aggregation is now supported in six new Regions. For more information, see <a href="#">Multi-Account Multi-Region Data Aggregation</a> (p. 3262).</p>	October 4, 2018
AWS Config supports resource-level permissions for AWS Config Rules APIs actions	<p>With this release, AWS Config supports resource-level permissions for certain AWS Config Rules API actions. For more information about the supported APIs, see <a href="#">Supported Resource-Level Permissions for AWS Config Rules APIs Actions</a> (p. 3287).</p>	October 1, 2018
AWS Config supports CodePipeline resource type	<p>With this release, you can use AWS Config to record configuration changes to the AWS CodePipeline resource type. For more information, see <a href="#">Supported Resource Types</a> (p. 9).</p>	September 12, 2018

Change	Description	Release Date
AWS Config supports new managed rules	<p>This release supports the following new managed rules:</p> <ul style="list-style-type: none"> <li>• <a href="#">ec2-instance-managed-by-systems-manager</a> (p. 132)</li> <li>• <a href="#">ec2-managedinstance-association-compliance-status-check</a> (p. 135)</li> <li>• <a href="#">ec2-managedinstance-patch-compliance-status-check</a> (p. 136)</li> <li>• <a href="#">guardduty-enabled-centralized</a> (p. 152)</li> <li>• <a href="#">rds-snapshots-public-prohibited</a> (p. 168)</li> <li>• <a href="#">s3-bucket-blacklisted-actions-prohibited</a> (p. 176)</li> <li>• <a href="#">s3-bucket-policy-not-more-permissive</a> (p. 179)</li> </ul> <p>For more information, see <a href="#">List of AWS Config Managed Rules</a> (p. 103).</p>	September 5, 2018
AWS Config supports AWS Systems Manager resource type	<p>With this release, you can use AWS Config to record configuration changes to the AWS Systems Manager patch compliance and association compliance resource types. For more information, see <a href="#">Supported Resource Types</a> (p. 9).</p>	August 9, 2018
AWS Config allows you to delete your AWS Config data using AWS Management Console	<p>With this release, AWS Config introduces support for retention period using AWS Management Console. In the AWS Management Console, you can select a custom data retention period for your <code>ConfigurationItems</code>. For more information, see <a href="#">Deleting AWS Config Data</a> (p. 80).</p>	August 7, 2018
AWS Config supports AWS Shield resource type	<p>With this release, you can use AWS Config to record configuration changes to the AWS Shield Protection resource type. For more information, see <a href="#">Supported Resource Types</a> (p. 9).</p>	August 7, 2018
AWS Config supports AWS PrivateLink	<p>With this release, AWS Config supports AWS PrivateLink, enabling you to route data between your Amazon Virtual Private Cloud (VPC) and AWS Config entirely within the AWS network. For more information, see <a href="#">Using AWS Config with Interface Amazon VPC Endpoints</a> (p. 3318).</p>	July 31, 2018

Change	Description	Release Date
AWS Config allows you to delete your AWS Config data	<p>With this release, AWS Config introduces support for retention period. AWS Config allows you to delete your data by specifying a retention period for your <code>ConfigurationItems</code>. For more information, see <a href="#">Deleting AWS Config Data (p. 80)</a>.</p> <p>With this release, AWS Config adds the following new APIs. For more information, see the <i>AWS Config API Reference</i> :</p> <ul style="list-style-type: none"> <li>• <a href="#">PutRetentionConfiguration</a></li> <li>• <a href="#">DescribeRetentionConfigurations</a></li> <li>• <a href="#">DeleteRetentionConfiguration</a></li> </ul>	May 25, 2018
AWS Config supports new managed rules	<p>This release supports the following two new managed rules:</p> <ul style="list-style-type: none"> <li>• <a href="#">lambda-function-settings-check (p. 162)</a></li> <li>• <a href="#">s3-bucket-replication-enabled (p. 180)</a></li> <li>• <a href="#">iam-policy-blacklisted-check (p. 155)</a></li> </ul> <p>For more information, see <a href="#">List of AWS Config Managed Rules (p. 103)</a>.</p>	May 10, 2018
AWS Config supports AWS X-Ray resource type	<p>With this release, you can use AWS Config to record configuration changes to the AWS X-Ray <code>EncryptionConfig</code> resource type. For more information, see <a href="#">Supported Resource Types (p. 9)</a>.</p>	May 1, 2018
AWS Config supports AWS Lambda resource type and one new managed rule	<p>With this release, you can use AWS Config to record configuration changes to the AWS Lambda function resource type. For more information, see <a href="#">Supported Resource Types (p. 9)</a>.</p> <p>This release also supports the <a href="#">lambda-function-public-access-prohibited (p. 161)</a> managed rule. For more information, see <a href="#">AWS Config Managed Rules (p. 102)</a>.</p>	April 25, 2018

Change	Description	Release Date
AWS Config supports AWS Elastic Beanstalk resource type	<p>With this release, you can use AWS Config to record configuration changes to the AWS Elastic Beanstalk Application, Application Version, and Environment resources.</p> <p>For more information, see <a href="#">Supported Resource Types (p. 9)</a>.</p>	April 24, 2018
AWS Config supports new managed rules	<p>This release supports the following two new managed rules:</p> <ul style="list-style-type: none"> <li>• <a href="#">fms-webacl-resource-policy-check (p. 150)</a></li> <li>• <a href="#">fms-webacl-rulegroup-association-check (p. 151)</a></li> </ul> <p>For more information, see <a href="#">List of AWS Config Managed Rules (p. 103)</a>.</p>	April 4, 2018
Multi-account multi-region data aggregation	<p>With this release, AWS Config introduces multi-account multi-region data aggregation. This feature allows you to aggregate AWS Config data from multiple accounts or an organization and multiple regions into an aggregator account. For more information, see <a href="#">Multi-Account Multi-Region Data Aggregation (p. 3262)</a>.</p> <p>With this release, AWS Config adds the following new APIs. For more information, see the <i>AWS Config API Reference</i> :</p> <ul style="list-style-type: none"> <li>• <a href="#">PutConfigurationAggregator</a></li> <li>• <a href="#">DescribePendingAggregationRequests</a></li> <li>• <a href="#">DeletePendingAggregationRequest</a></li> <li>• <a href="#">PutAggregationAuthorization</a></li> <li>• <a href="#">DescribeAggregationAuthorizations</a></li> <li>• <a href="#">GetAggregateConfigRuleComplianceSummary</a></li> <li>• <a href="#">DescribeAggregateComplianceByConfigRules</a></li> <li>• <a href="#">GetAggregateComplianceDetailsByConfigRule</a></li> <li>• <a href="#">DescribeConfigurationAggregators</a></li> <li>• <a href="#">DescribeConfigurationAggregatorSourcesStatus</a></li> <li>• <a href="#">DeleteAggregationAuthorization</a></li> <li>• <a href="#">DeleteConfigurationAggregator</a></li> </ul>	April 4, 2018

Change	Description	Release Date
Monitoring AWS Config with Amazon CloudWatch Events	<p>With this release, use Amazon CloudWatch Events to detect and react to changes in the status of AWS Config events.</p> <p>For more information, see <a href="#">Monitoring AWS Config with Amazon CloudWatch Events</a> (p. 3316).</p>	March 29, 2018
New API operation	<p>With this release, AWS Config adds support for <a href="#">BatchGetResourceConfig</a> API, allowing you to batch-retrieve the current state of one or more of your resources.</p>	March 20, 2018
AWS Config supports AWS WAF RuleGroup resource type	<p>With this release, you can use AWS Config to record configuration changes to the AWS WAF RuleGroup and AWS WAF RuleGroup Regional resources.</p> <p>For more information, see <a href="#">Supported Resource Types</a> (p. 9).</p>	February 15, 2018
AWS Config supports new managed rules	<p>This release supports the following new managed rules:</p> <ul style="list-style-type: none"> <li>• <a href="#">elb-acm-certificate-required</a> (p. 143)</li> <li>• <a href="#">elb-custom-security-policy-ssl-check</a> (p. 143)</li> <li>• <a href="#">elb-predefined-security-policy-ssl-check</a> (p. 145)</li> <li>• <a href="#">codebuild-project-envvar-awscred-check</a> (p. 123)</li> <li>• <a href="#">codebuild-project-source-repo-url-check</a> (p. 123)</li> <li>• <a href="#">iam-group-has-users-check</a> (p. 153)</li> <li>• <a href="#">s3-bucket-server-side-encryption-enabled</a> (p. 181)</li> </ul> <p>For more information, see <a href="#">List of AWS Config Managed Rules</a> (p. 103).</p>	January 25, 2018
AWS Config supports Elastic Load Balancing resource type	<p>With this release, you can use AWS Config to record configuration changes to your Elastic Load Balancing classic load balancers.</p> <p>For more information, see <a href="#">Supported Resource Types</a> (p. 9).</p>	November 17, 2017

Change	Description	Release Date
<p>AWS Config supports the Amazon CloudFront and AWS WAF resource type</p>	<p>With this release, you can use AWS Config to record configuration changes to your CloudFront distribution and streaming distribution.</p> <p>With this release, you can use AWS Config to record configuration changes to the following AWS WAF and AWS WAF Regional resources; rate based rule, rule, and Web ACL.</p> <p>For more information, see <a href="#">Supported Resource Types (p. 9)</a>.</p>	<p>November 15, 2017</p>
<p>AWS Config supports the AWS CodeBuild resource type</p>	<p>With this release, you can use AWS Config to record configuration changes to your AWS CodeBuild projects.</p> <p>For more information, see <a href="#">Supported Resource Types (p. 9)</a>.</p>	<p>October 20, 2017</p>
<p>AWS Config supports Auto Scaling resources and one new managed rule</p>	<p>With this release, you can use AWS Config to record configuration changes to the following Auto Scaling resources; groups, launch configuration, scheduled action, and scaling policy.</p> <p>For more information, see <a href="#">Supported Resource Types (p. 9)</a>.</p> <p>This release also supports the following managed rule:</p> <ul style="list-style-type: none"> <li>• <a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a></li> </ul> <p>For more information, see <a href="#">AWS Config Managed Rules (p. 102)</a>.</p>	<p>September 18, 2017</p>
<p>AWS Config supports the AWS CodeBuild resource type</p>	<p>With this release, you can use AWS Config to record configuration changes to your AWS CodeBuild projects.</p> <p>For more information, see <a href="#">Supported Resource Types (p. 9)</a>.</p>	<p>October 20, 2017</p>

Change	Description	Release Date
<p>AWS Config supports Auto Scaling resources and one new managed rule</p>	<p>With this release, you can use AWS Config to record configuration changes to the following Auto Scaling resources; groups, launch configuration, scheduled action, and scaling policy.</p> <p>For more information, see <a href="#">Supported Resource Types (p. 9)</a>.</p> <p>This release also supports the following managed rule:</p> <ul style="list-style-type: none"> <li>• <a href="#">autoscaling-group-elb-healthcheck-required (p. 113)</a></li> </ul> <p>For more information, see <a href="#">AWS Config Managed Rules (p. 102)</a>.</p>	<p>September 18, 2017</p>
<p>AWS Config supports the DynamoDB table resource type and one new managed rule</p>	<p>With this release, you can use AWS Config to record configuration changes to your DynamoDB tables.</p> <p>For more information, see <a href="#">Supported Resource Types (p. 9)</a>.</p> <p>This release supports the following managed rule:</p> <ul style="list-style-type: none"> <li>• <a href="#">dynamodb-autoscaling-enabled (p. 128)</a></li> </ul> <p>For more information, see <a href="#">AWS Config Managed Rules (p. 102)</a>.</p>	<p>September 8, 2017</p>
<p>AWS Config supports two new managed rules for Amazon S3</p>	<p>This release supports two new managed rules:</p> <ul style="list-style-type: none"> <li>• <a href="#">s3-bucket-public-read-prohibited (p. 179)</a></li> <li>• <a href="#">s3-bucket-public-write-prohibited (p. 180)</a></li> </ul> <p>For more information, see <a href="#">AWS Config Managed Rules (p. 102)</a>.</p>	<p>August 14, 2017</p>

Change	Description	Release Date
New page in the AWS Config console	<p>You can use the <b>Dashboard</b> in the AWS Config console to see the following:</p> <ul style="list-style-type: none"> <li>• Total number of resources</li> <li>• Total number of rules</li> <li>• Number of noncompliant resources</li> <li>• Number of noncompliant rules</li> </ul> <p>For more information, see <a href="#">Viewing the AWS Config Dashboard (p. 33)</a>.</p>	July 17, 2017
New API operation	<p>You can use the <a href="#">GetDiscoveredResourceCounts</a> operation to return the number of resource types, the number of each resource type, and the total number of resources that AWS Config is recording in a Region for your AWS account.</p>	July 17, 2017
AWS Config supports the AWS CloudFormation stack resource type and one new managed rule	<p>With this release, you can use AWS Config to record configuration changes to your AWS CloudFormation stacks.</p> <p>For more information, see <a href="#">Supported Resource Types (p. 9)</a>.</p> <p>This release supports the following managed rule:</p> <ul style="list-style-type: none"> <li>• <a href="#">cloudformation-stack-notification-check (p. 114)</a></li> </ul> <p>For more information, see <a href="#">AWS Config Managed Rules (p. 102)</a>.</p>	July 6, 2017
New and updated content	<p>This release adds support for AWS Config Rules in the Canada (Central) Region and South America (São Paulo) Region.</p> <p>For all regions that support AWS Config and Config Rules, see <a href="#">AWS Regions and Endpoints</a> in the <i>AWS General Reference</i>.</p>	July 5, 2017
New and updated content	<p>AWS Config Rules is available in the AWS GovCloud (US) Region. For more information, see the <a href="#">AWS GovCloud (US) User Guide</a>.</p> <p>For regions that support AWS Config, see <a href="#">AWS Regions and Endpoints</a> in the <i>AWS General Reference</i>.</p>	June 8, 2017

Change	Description	Release Date
<p>AWS Config supports the Amazon CloudWatch alarm resource type and three new managed rules</p>	<p>With this release, you can use AWS Config to record configuration changes to your Amazon CloudWatch alarms.</p> <p>For more information, see <a href="#">Supported Resource Types (p. 9)</a>.</p> <p>This release supports three new managed rules:</p> <ul style="list-style-type: none"> <li>• <a href="#">cloudwatch-alarm-action-check (p. 119)</a></li> <li>• <a href="#">cloudwatch-alarm-resource-check (p. 120)</a></li> <li>• <a href="#">cloudwatch-alarm-settings-check (p. 120)</a></li> </ul> <p>For more information, see <a href="#">AWS Config Managed Rules (p. 102)</a>.</p>	<p>June 1, 2017</p>
<p>New and updated content</p>	<p>This release supports specifying the application version number for the following managed rules:</p> <ul style="list-style-type: none"> <li>• <a href="#">ec2-managedinstance-applications-blacklisted (p. 134)</a></li> <li>• <a href="#">ec2-managedinstance-applications-required (p. 134)</a></li> </ul> <p>For more information, see <a href="#">AWS Config Managed Rules (p. 102)</a>.</p>	<p>June 1, 2017</p>
<p>New and updated content</p>	<p>This release adds support for AWS Config Rules in the Asia Pacific (Mumbai) Region. For more information, see <a href="#">AWS Regions and Endpoints</a> in the <i>AWS General Reference</i>.</p>	<p>April 27, 2017</p>
<p>New and updated content</p>	<p>This release supports an updated console experience for adding AWS Config managed rules to your account for the first time.</p> <p>When you set up AWS Config Rules for the first time or in a new Region, you can search for AWS managed rules by name, description, or label. You can choose <b>Select all</b> to select all rules or choose <b>Clear all</b> to clear all rules.</p> <p>For more information, see <a href="#">Setting Up AWS Config Rules with the Console (p. 33)</a>.</p>	<p>April 5, 2017</p>

Change	Description	Release Date
AWS Config supports new managed rules	<p>This release supports the following new managed rules:</p> <ul style="list-style-type: none"> <li>• <a href="#">acm-certificate-expiration-check</a> (p. 108)</li> <li>• <a href="#">ec2-instance-detailed-monitoring-enabled</a> (p. 132)</li> <li>• <a href="#">ec2-managedinstance-inventory-blacklisted</a> (p. 135)</li> <li>• <a href="#">ec2-volume-inuse-check</a> (p. 137)</li> <li>• <a href="#">iam-user-group-membership-check</a> (p. 157)</li> <li>• <a href="#">iam-user-no-policies-check</a> (p. 158)</li> <li>• <a href="#">s3-bucket-ssl-requests-only</a> (p. 181)</li> </ul> <p>For more information, see <a href="#">List of AWS Config Managed Rules</a> (p. 103).</p>	February 21, 2017
New and updated content	<p>This release adds support for AWS Config Rules in the Europe (London) Region. For more information, see <a href="#">AWS Regions and Endpoints</a> in the <i>AWS General Reference</i>.</p>	February 21, 2017
New and updated content	<p>This release adds AWS CloudFormation templates for AWS Config managed rules. You can use the templates to create managed rules for your account. For more information, see <a href="#">Creating AWS Config Managed Rules With AWS CloudFormation Templates</a> (p. 192).</p>	February 16, 2017
New and updated content	<p>This release adds support for a new test mode for the <code>PutEvaluations</code> API. Set the <code>TestMode</code> parameter to true in your custom rule to verify whether your AWS Lambda function will deliver evaluation results to AWS Config. No updates occur to your existing evaluations, and evaluation results are not sent to AWS Config.</p> <p>For more information, see <a href="#">PutEvaluations</a> in the <i>AWS Config API Reference</i>.</p>	February 16, 2017
New and updated content	<p>This release adds support for AWS Config Rules in the Asia Pacific (Seoul), and US West (N. California) Regions. For more information, see <a href="#">AWS Regions and Endpoints</a> in the <i>AWS General Reference</i>.</p>	December 21, 2016

Change	Description	Release Date
New and updated content	This release adds support for AWS Config in the Europe (London) Region. For more information, see <a href="#">AWS Regions and Endpoints</a> in the <i>AWS General Reference</i> .	December 13, 2016
New and updated content	This release adds support for AWS Config in the Canada (Central) Region. For more information, see <a href="#">AWS Regions and Endpoints</a> in the <i>AWS General Reference</i> .	December 8, 2016
AWS Config supports Amazon Redshift resource types and two new managed rules	<p>With this release, you can use AWS Config to record configuration changes to your Amazon Redshift clusters, cluster parameter groups, cluster security groups, cluster snapshots, cluster subnet groups, and event subscriptions.</p> <p>For more information, see <a href="#">Supported Resource Types (p. 9)</a>.</p> <p>This release supports two new managed rules:</p> <ul style="list-style-type: none"> <li>• <a href="#">redshift-cluster-configuration-check (p. 170)</a></li> <li>• <a href="#">redshift-cluster-maintenancesettings-check (p. 171)</a></li> </ul> <p>For more information, see <a href="#">List of AWS Config Managed Rules (p. 103)</a>.</p>	December 7, 2016
New and updated content	<p>This release adds support for a new managed rule:</p> <ul style="list-style-type: none"> <li>• <a href="#">dynamodb-throughput-limit-check (p. 130)</a></li> </ul> <p>For more information, see <a href="#">List of AWS Config Managed Rules (p. 103)</a>.</p>	December 7, 2016
New and updated content	This release adds support for creating up to 50 rules per Region in an account. For more information, see <a href="#">AWS Config Limits</a> in the <i>AWS General Reference</i> .	December 7, 2016

Change	Description	Release Date
<p>AWS Config supports the managed instance inventory resource type for Amazon EC2 Systems Manager and three new managed rules</p>	<p>With this release, you can use AWS Config to record software configuration changes on your managed instances with support for managed instance inventory.</p> <p>For more information, see <a href="#">Recording Software Configuration for Managed Instances</a> (p. 65).</p> <p>This release supports three new managed rules:</p> <ul style="list-style-type: none"> <li>• <a href="#">ec2-managedinstance-inventory-blacklisted</a> (p. 135)</li> <li>• <a href="#">ec2-managedinstance-applications-required</a> (p. 134)</li> <li>• <a href="#">ec2-managedinstance-platform-check</a> (p. 136)</li> </ul> <p>For more information, see <a href="#">List of AWS Config Managed Rules</a> (p. 103).</p>	<p>December 1, 2016</p>
<p>AWS Config supports the Amazon S3 bucket resource and two new managed rules</p>	<p>With this release, you can use AWS Config to record configuration changes to your Amazon S3 buckets. For more information, see <a href="#">Supported Resource Types</a> (p. 9).</p> <p>This release supports two new managed rules:</p> <ul style="list-style-type: none"> <li>• <a href="#">s3-bucket-logging-enabled</a> (p. 177)</li> <li>• <a href="#">s3-bucket-versioning-enabled</a> (p. 181)</li> </ul> <p>For more information, see <a href="#">AWS Config Managed Rules</a> (p. 102).</p>	<p>October 18, 2016</p>
<p>New and updated content</p>	<p>This release adds support for AWS Config and AWS Config Rules in the US East (Ohio) Region. For more information, see <a href="#">AWS Regions and Endpoints</a> in the <i>AWS General Reference</i>.</p>	<p>October 17, 2016</p>

Change	Description	Release Date
New and updated managed rules	<p>This update adds support for eight new managed rules:</p> <ul style="list-style-type: none"> <li>• <a href="#">approved-amis-by-id</a> (p. 112)</li> <li>• <a href="#">approved-amis-by-tag</a> (p. 112)</li> <li>• <a href="#">db-instance-backup-enabled</a> (p. 126)</li> <li>• <a href="#">desired-instance-type</a> (p. 127)</li> <li>• <a href="#">ebs-optimized-instance</a> (p. 131)</li> <li>• <a href="#">iam-password-policy</a> (p. 154)</li> <li>• <a href="#">rds-multi-az-support</a> (p. 168)</li> <li>• <a href="#">rds-storage-encrypted</a> (p. 169)</li> </ul> <p>You can specify multiple parameter values for the following rules:</p> <ul style="list-style-type: none"> <li>• <a href="#">desired-instance-tenancy</a> (p. 126)</li> <li>• <a href="#">required-tags</a> (p. 172)</li> </ul> <p>For more information, see <a href="#">List of AWS Config Managed Rules</a> (p. 103).</p>	October 4, 2016
New and updated content for the AWS Config console	<p>This update adds support for viewing AWS CloudTrail API activity in the AWS Config timeline. If CloudTrail is logging for your account, you can view create, update, and delete API events for configuration changes to your resources. For more information, see <a href="#">Viewing Configuration Details</a> (p. 45).</p>	September 06, 2016
AWS Config supports Elastic Load Balancing resource type	<p>With this release, you can use AWS Config to record configuration changes to your Elastic Load Balancing application load balancers. For more information, see <a href="#">Supported Resource Types</a> (p. 9).</p>	August 31, 2016
New and updated content	<p>This release adds support for AWS Config Rules in the Asia Pacific (Singapore), and Asia Pacific (Sydney) Regions. For more information, see <a href="#">AWS Regions and Endpoints</a> in the <i>AWS General Reference</i>.</p>	August 18, 2016

Change	Description	Release Date
New and updated content for AWS Config Rules	<p>This update adds support for creating a rule that can be triggered by both configuration changes and at a periodic frequency that you choose. For more information, see <a href="#">Specifying Triggers for AWS Config Rules (p. 101)</a>.</p> <p>This update also adds support for manually evaluating your resources against your rule and deleting evaluation results. For more information, see <a href="#">Evaluating Your Resources (p. 210)</a>.</p> <p>This update also adds support for evaluating additional resource types using custom rules. For more information, see <a href="#">Evaluating Additional Resource Types (p. 198)</a>.</p>	July 25, 2016
AWS Config supports Amazon RDS and AWS Certificate Manager (ACM) resource types	<p>With this release, you can use AWS Config to record configuration changes to your Amazon Relational Database Service (Amazon RDS) DB instances, DB security groups, DB snapshots, DB subnet groups, and event subscriptions. You can also use AWS Config to record configuration changes to certificates provided by ACM.</p> <p>For more information, see <a href="#">Supported Resource Types (p. 9)</a>.</p>	July 21, 2016
Updated information about managing the configuration recorder	<p>This update adds steps for renaming and deleting the configuration recorder to <a href="#">Managing the Configuration Recorder (p. 60)</a>.</p>	July 07, 2016
Simplified role creation and updated policies	<p>With this update, creating an IAM role for AWS Config is simplified. This enhancement is available in regions that support Config rules. To support this enhancement, the steps in <a href="#">Setting Up AWS Config with the Console (p. 25)</a> are updated, the example policy in <a href="#">Permissions for the Amazon S3 Bucket (p. 3292)</a> is updated, and the example policy in <a href="#">Granting Custom Permissions for AWS Config Users (p. 3281)</a> is updated.</p>	March 31, 2016

Change	Description	Release Date
Example functions and events for Config rules	This update provides updated example functions in <a href="#">Example AWS Lambda Functions for AWS Config Rules (Node.js)</a> (p. 199), and this update adds example events in <a href="#">Example Events for AWS Config Rules</a> (p. 204).	March 29, 2016
AWS Config Rules GitHub repository	This update adds information about the <a href="#">AWS Config Rules GitHub repository</a> to <a href="#">Evaluating Resources with AWS Config Rules</a> (p. 96). This repository provides sample functions for custom rules that are developed and contributed by AWS Config users.	March 1, 2016
AWS Config Rules	This release introduces AWS Config Rules. With rules, you can use AWS Config to evaluate whether your AWS resources comply with your desired configurations. For more information, see <a href="#">Evaluating Resources with AWS Config Rules</a> (p. 96).	December 18, 2015
AWS Config supports IAM resource types	With this release, you can use AWS Config to record configuration changes to your IAM users, groups, roles, and customer managed policies. For more information, see <a href="#">Supported Resource Types</a> (p. 9).	December 10, 2015
AWS Config supports EC2 Dedicated host	With this release, you can use AWS Config to record configuration changes to your EC2 Dedicated hosts. For more information, see <a href="#">Supported Resource Types</a> (p. 9).	November 23, 2015
Updated permissions information	This update adds information about the following AWS managed policies for AWS Config: <ul style="list-style-type: none"> <li>• <a href="#">AWS_ConfigRole</a> – Grants AWS Config permission to get configuration details about your resources. For more information, see <a href="#">IAM Role Policy for Getting Configuration Details</a> (p. 3291).</li> <li>• <a href="#">AWSConfigUserAccess</a> – Grants read-only access to an AWS Config user. For more information, see <a href="#">Granting Custom Permissions for AWS Config Users</a> (p. 3281).</li> </ul>	October 19, 2015

Change	Description	Release Date
AWS Config Rules preview	This release introduces the AWS Config Rules preview. With rules, you can use AWS Config to evaluate whether your AWS resources comply with your desired configurations. For more information, see <a href="#">Evaluating Resources with AWS Config Rules (p. 96)</a> .	October 7, 2015
New and updated content	This release adds the ability to look up resources that AWS Config has discovered. For more information, see <a href="#">Looking Up Resources That Are Discovered by AWS Config (p. 44)</a> .	August 27, 2015
New and updated content	This release adds the ability to select which resource types AWS Config records. For more information, see <a href="#">Selecting Which Resources AWS Config Records (p. 62)</a> .	June 23, 2015
New and updated content	This release adds support for the following regions: Asia Pacific (Tokyo), Asia Pacific (Singapore), Europe (Frankfurt), South America (São Paulo), and US West (N. California). For more information, see <a href="#">AWS Regions and Endpoints</a> .	April 6, 2015
New guide	This release introduces AWS Config.	November 12, 2014

# AWS glossary

For the latest AWS terminology, see the [AWS glossary](#) in the *AWS General Reference*.