aws

User Guide

AWS Audit Manager

AWS Audit Manager: User Guide

Table of Contents

What is AWS Audit Manager?

Welcome to the AWS Audit Manager User Guide.

AWS Audit Manager helps you continually audit your AWS usage to simplify how you manage risk and compliance with regulations and industry standards. Audit Manager automates evidence collection so you can more easily assess whether your policies, procedures, and activities—also known as *controls*—are operating effectively. When it's time for an audit, Audit Manager helps you manage stakeholder reviews of your controls. This means that you can build audit-ready reports with much less manual effort.

Audit Manager provides prebuilt frameworks that structure and automate assessments for a given compliance standard or regulation. Frameworks include a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped according to the requirements of the specified compliance standard or regulation. You can also customize frameworks and controls to support internal audits according to your specific requirements.

You can create an assessment from any framework. When you create an assessment, Audit Manager automatically runs resource assessments. These assessments collect data for the AWS accounts that you define as in scope for your audit. The data that's collected is automatically transformed into audit-friendly evidence. Then, it's attached to the relevant controls to help you demonstrate compliance in security, change management, business continuity, and software licensing. This evidence collection process is ongoing, and starts when you create your assessment. After you complete an audit and you no longer need Audit Manager to collect evidence, you can stop evidence collection. To do this, change the status of your assessment to *inactive*.

Features of Audit Manager

With AWS Audit Manager, you can do the following tasks:

- **Get started quickly** — Create your first assessment by selecting from a gallery of prebuilt frameworks that support a range of compliance standards and regulations. Then, initiate automatic evidence collection to audit your AWS service usage.
- **Upload and manage evidence from hybrid or multicloud environments** — In addition to the evidence that Audit Manager collects from your AWS environment, you can also upload and centrally manage evidence from your on-premises or multicloud environment.

- **Support common compliance standards and regulations** — Choose one of the AWS Audit Manager standard frameworks. These frameworks provide prebuilt control mappings for common compliance standards and regulations. These include the CIS Foundation Benchmark, PCI DSS, GDPR, HIPAA, SOC2, GxP, and AWS operational best practices.
- **Monitor your active assessments** — Use the Audit Manager dashboard to view analytics data for your active assessments, and quickly identify non-compliant evidence that needs to be remediated.
- **Search for evidence** — Use the Evidence finder feature to quickly find evidence that's relevant to your search query. You can generate an assessment report from your search results, or export your search results in CSV format.
- **Create custom controls** — Create your own control from scratch or make an editable copy of an existing standard control or custom control. You can also use the custom controls feature to create risk assessment questions and store the responses to those questions as manual evidence.
- **Map your enterprise controls to predefined groupings of AWS data sources** — Choose the common controls that represent your goals, and use them to create custom controls that collect evidence for your portfolio of compliance needs.
- **Create custom frameworks** — Create your own frameworks with standard or custom controls based on your specific requirements for internal audits.
- **Share custom frameworks** — Share your custom Audit Manager frameworks with another AWS account, or replicate them into another AWS Region under your own account.
- **Support cross-team collaboration** — Delegate control sets to subject matter experts who can review related evidence, add comments, and update the status of each control.
- **Create reports for auditors** — Generate assessment reports that summarize the relevant evidence that's collected for your audit and link to folders that contain the detailed evidence.
- **Ensure evidence integrity** — Store evidence in a secure location, where it remains unaltered.

> **Note**
>
> AWS Audit Manager assists in collecting evidence that's relevant for verifying compliance with specific compliance standards and regulations. However, it doesn't assess your compliance itself. The evidence that's collected through AWS Audit Manager therefore might not include all the information about your AWS usage that's needed for audits. AWS Audit Manager isn't a substitute for legal counsel or compliance experts.

Pricing for Audit Manager

For more information about pricing, see AWS Audit Manager Pricing.

Are you a first-time user of Audit Manager?

If you're a first-time user of Audit Manager, we recommend that you start with the following pages:

1. Understanding AWS Audit Manager concepts and terminology – Learn about the key concepts and terms used in Audit Manager, such as assessments, frameworks, and controls.
2. Understanding how AWS Audit Manager collects evidence – Learn about how Audit Manager gathers evidence for a resource assessment.
3. Setting up AWS Audit Manager with the recommended settings – Learn about the setup requirements for Audit Manager.
4. Getting started with AWS Audit Manager – Follow a tutorial to create your first Audit Manager assessment.
5. AWS Audit Manager API Reference – Familiarize yourself with the Audit Manager API actions and data types.

Related AWS services

AWS Audit Manager integrates with multiple AWS services to automatically collect evidence that you can include in your assessment reports.

AWS Security Hub

AWS Security Hub monitors your environment using automated security checks that are based on AWS best practices and industry standards. Audit Manager captures snapshots of your resource security posture by reporting the results of security checks directly from Security Hub. For more information about Security Hub, see What is AWS Security Hub? in the *AWS Security Hub User Guide*.

AWS CloudTrail

AWS CloudTrail helps you monitor the calls made to AWS resources in your account. These include calls made by the AWS Management Console, the AWS CLI, and other AWS services. Audit

Manager collects log data from CloudTrail directly, and converts the processed logs into user activity evidence. For more information about CloudTrail, see What is AWS CloudTrail? in the *AWS CloudTrail User Guide*.

AWS Config

AWS Config provides a detailed view of the configuration of AWS resources in your AWS account. This includes information about how resources are related to one another and how they were configured in the past. Audit Manager captures snapshots of your resource security posture by reporting findings directly from AWS Config. For more information about AWS Config, see What is AWS Config? in the *AWS Config User Guide*.

AWS License Manager

AWS License Manager streamlines the process of bringing software vendor licenses to the cloud. As you build out cloud infrastructure on AWS, you can save costs by repurposing your existing license inventory for use with cloud resources. Audit Manager provides a License Manager framework to assist you with your audit preparation. This framework is integrated with License Manager to aggregate license usage information based on customer defined licensing rules. For more information on License Manager, see What is AWS License Manager? in the *AWS License Manager User Guide*.

AWS Control Tower

AWS Control Tower enforces preventative and detective guardrails for cloud infrastructure. Audit Manager provides an AWS Control Tower Guardrails framework to assist you with your audit preparation. This framework contains all of the AWS Config rules that are based on guardrails from AWS Control Tower. For more information about AWS Control Tower, see What is AWS Control Tower? in the *AWS Control Tower User Guide*.

AWS Artifact

AWS Artifact is a self-service audit artifact retrieval portal that provides on-demand access to the compliance documentation and certifications for AWS infrastructure. AWS Artifact offers evidence to prove that the AWS Cloud infrastructure meets the compliance requirements. In contrast, AWS Audit Manager helps you collect, review, and manage evidence to demonstrate that your usage of AWS services is in compliance. For more information about AWS Artifact, see What is AWS Artifact? in the *AWS Artifact User Guide*. You can download a list of AWS reports in the AWS Management Console.

Amazon EventBridge

Amazon EventBridge helps you automate your AWS services and respond automatically to system events such as application availability issues or resource changes. You can use EventBridge rules to detect and react to Audit Manager events. Based on the rules that you create, EventBridge invokes one or more target actions when an event matches the values that you specify in a rule. For more information, see Monitoring AWS Audit Manager with Amazon EventBridge.

For a list of AWS services in scope of specific compliance programs, see AWS services in Scope by Compliance Program. For more general information, see AWS Compliance Programs.

More Audit Manager resources

Explore the following resources to learn more about Audit Manager.

- Collect Evidence and Manage Audit Data Using AWS Audit Manager
- Integrate across the Three Lines Model (Part 2): Transform AWS Config conformance packs into AWS Audit Manager assessments from the *AWS Management & Governance Blog*

Understanding AWS Audit Manager concepts and terminology

To help you get started, this page defines terms and explains some of the key concepts of AWS Audit Manager.

A

| B | | | | | G | H | | J | K | L | M | N | O | P | Q | | | T | U | V | W | X | Y | Z

Assessment

You can use an Audit Manager assessment to automatically collect evidence that's relevant for an audit.

An assessment is based on a framework, which is a grouping of controls that are related to your audit. You can create an assessment from a standard framework or a custom framework. Standard frameworks contain prebuilt control sets that support a specific compliance standard or regulation. In contrast, custom frameworks contain controls that you can customize and group according to your specific audit requirements. Using a framework as a starting point, you

can create an assessment that specifies the AWS accounts that you want to include in the scope of your audit.

When you create an assessment, Audit Manager automatically starts to assess resources in your AWS accounts based on the controls that are defined in the framework. Next, it collects the relevant evidence and converts it into an auditor-friendly format. After doing this, it then attaches the evidence to the controls in your assessment. When it's time for an audit, you—or a delegate of your choice—can review the collected evidence and then add it to an assessment report. This assessment report helps you to demonstrate that your controls are working as intended.

Evidence collection is an ongoing process that starts when you create your assessment. You can stop evidence collection by changing the assessment status to *inactive*. Alternatively, you can stop evidence collection at the control level. You can do this by changing the status of a specific control within your assessment to *inactive*.

For instructions on how to create and manage assessments, see Managing assessments in AWS Audit Manager.

Assessment report

An assessment report is a finalized document that's generated from an Audit Manager assessment. These reports summarize the relevant evidence that's collected for your audit. They link to the relevant evidence folders. The folders are named and organized according to the controls that are specified in your assessment. For each assessment, you can review the evidence that Audit Manager collects, and decide which evidence you want to include in the assessment report.

To learn more about assessment reports, see Assessment reports. To learn how to generate an assessment report, see Preparing an assessment report in AWS Audit Manager.

Assessment report destination

An assessment report destination is the default S3 bucket where Audit Manager saves your assessment reports. To learn more, see Configuring your default assessment report destination.

Audit

An audit is an independent examination of the assets, operations, or business integrity of your organization. An information technology (IT) audit specifically examines the controls within the information systems of your organization. The goal of an IT audit is to determine if information systems safeguard assets, operate effectively, and maintain data integrity. All of these are

important to meeting the regulatory requirements that are mandated by a compliance standard or regulation.

Audit owner

The term *audit owner* has two different meanings depending on the context.

In the context of Audit Manager, an audit owner is a user or role that manages an assessment and its related resources. The responsibilities of this Audit Manager persona include creating assessments, reviewing evidence, and generating assessment reports. Audit Manager is a collaborative service, and audit owners benefit when other stakeholders participate in their assessments. For example, you can add other audit owners to your assessment to share management tasks. Or, if you're an audit owner and you need help interpreting the evidence that was collected for a control, you can delegate that control set to a stakeholder who has subject matter expertise in that area. Such a person is known as a *delegate* persona.

In business terms, an audit owner is someone who coordinates and oversees the audit readiness efforts of their company, and presents evidence to an auditor. Typically, this is a governance, risk, and compliance (GRC) professional, such as a Compliance Officer or a GDPR Data Protection Officer. GRC professionals have the expertise and authority to manage audit preparation. More specifically, they understand compliance requirements, and can analyze, interpret, and prepare reporting data. However, other business roles can also assume the Audit Manager persona of an audit owner—not only GRC professionals take on this role. For example, you might choose to have your Audit Manager assessments set up and managed by a technical expert from one of the following teams:

- SecOps
- IT/DevOps
- Security Operations Center/Incident Response
- Similar teams that own, develop, remediate, and deploy cloud assets, and understand the cloud infrastructure of your organization

Who you choose to assign as an audit owner in your Audit Manager assessment depends greatly on your organization. It also depends on how you structure your security operations and the specifics of the audit. In Audit Manager, the same individual can assume the audit owner persona in one assessment, and the delegate persona in another.

No matter how you choose to use Audit Manager, you can manage the separation of duties across your organization using the audit owner/delegate persona and granting specific IAM

policies to each user. Through this two-step approach, Audit Manager ensures that you have full control over all of the specifics of an individual assessment. For more information, see Recommended policies for user personas in AWS Audit Manager.

AWS managed source

An AWS managed source is an evidence source that AWS maintains for you.

Each AWS managed source is a predefined grouping of data sources that maps to a specific common control or core control. When you use a common control as an evidence source, you automatically collect evidence for all the core controls that support that common control. You can also use individual core controls as an evidence source.

Whenever an AWS managed source is updated, the same updates are automatically applied to all custom controls that use that AWS managed source. This means that your custom controls collect evidence against the latest definitions of that evidence source. This helps you to ensure continuous compliance as the cloud compliance environment changes.

See also: customer managed source, evidence source.

C

| B | | | | | G | H | | J | K | L | M | N | O | P | Q | | | T | U | V | W | X | Y | Z

Changelog

For each control in an assessment, Audit Manager tracks user activity for that control. You can then review an audit trail of activities that are related to a specific control. For more information about which user activities are captured in the changelog, see Changelog tab.

Cloud compliance

Cloud compliance is the general principle that cloud-delivered systems must be compliant with the standards that are faced by cloud customers.

Common control

See control.

Compliance regulation

A compliance regulation is a law, rule, or other order that's prescribed by an authority, typically to regulate conduct. One example is GDPR.

Compliance standard

A compliance standard is a structured set of guidelines that detail the processes of an organization for maintaining accordance with established regulations, specifications, or legislation. Examples include PCI DSS and HIPAA.

Control

A control is a safeguard or countermeasure that's prescribed for an information system or an organization. Controls are designed to protect the confidentiality, integrity, and availability of your information, and to meet a set of defined requirements. They provide an assurance that your resources are operating as intended, your data is reliable, and your organization is compliant with applicable laws and regulations.

In Audit Manager, a control can also represent a question in a vendor risk assessment questionnaire. In this case, a control is a specific question that asks information about an organization's security and compliance posture.

Controls collect evidence continually when they're active in your Audit Manager assessments. You can also manually add evidence to any control. Each piece of evidence is a record that helps you to demonstrate compliance with the control's requirements.

Audit Manager provides the following types of controls:

Control type	Description
Common control	You can think of a common control as an action that helps you to fulfill a control objective. Because common controls aren't specific to any compliance standard, they help you to collect evidence that can support a range of overlapping compliance obligations. For example, let's say you have a control objective called *Data classification and handling*. To fulfill this objective, you could implement a common control called *Access controls* to monitor and detect unauthorized access to your resources. • *Automated common controls* collect evidence for you. They consist of a grouping of one or more related core controls. In turn, each of these core controls automatically collects relevant evidence from a predefined group

Control type	Description
	of AWS data sources. AWS manages these underlying data sources for you, and updates them whenever regulations and standards change and new data sources are identified. • *Manual common controls* require you to upload your own evidence. This is because they typically require the provision of physical records, or details about events that happen outside of your AWS environment. For this reason, there are often no AWS data sources that can produce evidence to support the manual common control's requirements. You can't edit a common control. However, you can use any common control as an evidence source when you create a custom control.
Core control	This is a prescriptive guideline for your AWS environment. You can think of a core control as an action that helps you to meet the requirements of a common control. For example, let's say you use a common control called *Access controls* to monitor unauthorized access to your resources. To support this common control, you could use the core control called *Block public read access in S3 buckets*. Because core controls aren't specific to any compliance standard, they collect evidence that can support a range of overlapping compliance obligations. Each core control uses one or more data sources to collect evidence about a specific AWS service. AWS manages these underlying data sources for you, and updates them whenever regulations and standards change and new data sources are identified. You can't edit a core control. However, you can use any core control as an evidence source when you create a custom control.

Control type	Description
Standard control	This is a prebuilt control that Audit Manager provides. You can use standard controls to assist you with audit preparation for a specific compliance standard. Each standard control is related to a specific standard framework in Audit Manager, and collects evidence that you can use to demonstrate compliance with that framework. Standard controls collect evidence from underlying data sources that AWS manages. These data sources are automatically updated whenever regulations and standards change and new data sources are identified. You can't edit standard controls. However, you can make an editable copy of any standard control.
Custom control	This is a control that you create in Audit Manager to meet your specific compliance requirements. You can create a custom control from scratch, or make an editable copy of an existing standard control. When you create a custom control, you can define specific evidence sources that determine where Audit Manager collects evidence from. After you create a custom control, you can edit that control or add it to a custom framework. You can also make an editable copy of any custom control.

Control domain

You can think of a control domain as a category of controls that's not specific to any compliance standard. An example of a control domain is *Data protection*.

Controls are often grouped by domain for simple organizational purposes. Each domain has multiple objectives.

Control domain groupings are one of the most powerful features of the Audit Manager dashboard. Audit Manager highlights the controls in your assessments that have non-compliant evidence, and groups them by control domain. This enables you to focus your remediation efforts on specific subject domains as you prepare for an audit.

Control objective

A control objective describes the goal of the common controls that fall underneath it. Each objective can have multiple common controls. If these common controls are implemented successfully, they'll help you to fulfill the objective.

Each control objective falls under a control domain. For example, the *Data protection* control domain might have a control objective named *Data classification and handling.* To support this control objective, you could use a common control called *Access controls* to monitor and detect unauthorized access to your resources.

Core control

See control.

Custom control

See control.

Customer managed source

A customer managed source is an evidence source that you define.

When you create a custom control in Audit Manager, you can use this option to create your own individual data sources. This gives you the flexibility to collect automated evidence from a business-specific resource, such as a custom AWS Config rule. You can also use this option if you want to add manual evidence to your custom control.

When you use customer managed sources, you are responsible for maintaining all of the data sources that you create.

See also: AWS managed source, evidence source.

D

| B | | | | | G | H | | J | K | L | M | N | O | P | Q | | | T | U | V | W | X | Y | Z

Data source

Audit Manager uses *data sources* to collect evidence for a control. A data source has the following properties:

- A **data source type** defines which type of data source Audit Manager collects evidence from.
  - For automated evidence, the type can be *AWS Security Hub*, *AWS Config*, *AWS CloudTrail*, or *AWS API calls*.
  - If you upload your own evidence, the type is *Manual*.
  - The Audit Manager API refers to a data source type as a sourceType.
- A **data source mapping** is a keyword that pinpoints where evidence is collected from for a given data source type.
  - For example, this might be the name of a CloudTrail event or the name of an AWS Config rule.
  - The Audit Manager API refers to a data source mapping as a sourceKeyword.
- A **data source name** labels the pairing of a data source type and mapping.
  - For standard controls, Audit Manager provides a default name.
  - For custom controls, you can provide your own name.
  - The Audit Manager API refers to a data source name as a sourceName.

A single control can have multiple data source types and multiple mappings. For example, one control might collect evidence from a mixture of data source types (such as AWS Config and Security Hub). Another control might have AWS Config as its only data source type, with multiple AWS Config rules as mappings.

The following table lists the automated data source types and shows examples of some corresponding mappings.

Data source type	Description	Mapping example
AWS Security Hub	Use this data source type to capture a snapshot of your resource security posture. Audit Manager uses the name of a Security Hub control as the mapping keyword, and reports the result of that security check directly from Security Hub.	`EC2.1`

Data source type	Description	Mapping example
AWS Config	Use this data source type to capture a snapshot of your resource security posture. Audit Manager uses the name of an AWS Config rule as the mapping keyword, and reports the result of that rule check directly from AWS Config.	`SNS_ENCRYPTED_KMS`
AWS CloudTrail	Use this data source type to track a specific user activity that's needed in your audit. Audit Manager uses the name of a CloudTrail event as the mapping keyword, and collects the related user activity from your CloudTrail logs.	`CreateAccessKey`
AWS API calls	Use this data source type to take a snapshot of your resource configuration through an API call to a specific AWS service. Audit Manager uses the name of API call as the mapping keyword, and collects the API response.	`kms_ListKeys`

Delegate

A delegate is an AWS Audit Manager user with limited permissions. Delegates typically have specialized business or technical expertise. For example, these expertise might be in data retention policies, training plans, network infrastructure, or identity management. Delegates help audit owners review collected evidence for controls that are in their area of expertise. Delegates can review control sets and their related evidence, add comments, upload additional evidence, and update the status of each of the controls that you assign to them for review.

Audit owners assign specific control sets to delegates, not entire assessments. As a result, delegates have limited access to assessments. For instructions on how to delegate a control set, see Delegations in AWS Audit Manager.

E

| B | | | | | G | H | | J | K | L | M | N | O | P | Q | | | T | U | V | W | X | Y | Z

Evidence

Evidence is a record that contains the information that's needed to demonstrate compliance with a control's requirements. Examples of evidence include a change activity invoked by a user, and a system configuration snapshot.

There are two main types of evidence in Audit Manager: *automated evidence* and *manual evidence*.

Evidence type	Description
Automated evidence	This is the evidence that Audit Manager collects automatically. This includes the following three categories of automated evidence: 1. **Compliance check** — The result of a compliance check is captured from AWS Security Hub, AWS Config, or both. Examples of compliance checks include a security check result from Security Hub for a PCI DSS control, and an AWS Config rule evaluation for a HIPAA control.

Evidence type	Description
	For more information, see AWS Config Rules supported by AWS Audit Manager and AWS Security Hub controls supported by AWS Audit Manager. 2. **User activity**— User activity that changes a resource configuration is captured from CloudTrail logs as that activity occurs. Examples of user activities include a route table update, an Amazon RDS instance backup setting change, and an S3 bucket encryption policy change. For more information, see AWS CloudTrail event names supported by AWS Audit Manager. 3. **Configuration data** — A snapshot of the resource configuration is captured directly from an AWS service on a daily, weekly, or monthly basis. Examples of configuration snapshots include a list of routes for a VPC route table, an Amazon RDS instance backup setting, and an S3 bucket encryption policy. For more information, see AWS API calls supported by AWS Audit Manager.
Manual evidence	This is the evidence that you add to Audit Manager yourself. There are three ways to add your own evidence: 1. Import a file from Amazon S3 2. Upload a file from your browser 3. Enter a text response to a risk assessment question For more information, see Adding manual evidence in AWS Audit Manager.

Automated evidence collection starts when you create an assessment. This is an ongoing process, and Audit Manager collects evidence at different frequencies depending on the

evidence type and the underlying data source. For more information, see Understanding how AWS Audit Manager collects evidence.

For instructions on how to review evidence in an assessment, see Reviewing evidence in AWS Audit Manager.

Evidence source

An evidence source defines where a control collects evidence from. It can be an individual data source, or a predefined grouping of data sources that maps to a common control or a core control.

When you create a custom control, you can collect evidence from AWS managed sources, customer managed sources, or both.

> **Tip**
>
> We recommend that you use AWS managed sources. Whenever an AWS managed source is updated, the same updates are automatically applied to all custom controls that use these sources. This means that your custom controls always collect evidence against the latest definitions of that evidence source. This helps you to ensure continuous compliance as the cloud compliance environment changes.

See also: AWS managed source, customer managed source.

Evidence collection method

There are two ways that a control can collect evidence.

Evidence collection method	Description
Automated	Automated controls automatically collect evidence from AWS data sources. This automated evidence can help you to demonstrate full or partial compliance with the control.
Manual	Manual controls require you to upload your own evidence to demonstrate compliance with the control.

Note

You can attach manual evidence to any automated control. In many cases, a combination of automated and manual evidence is needed to demonstrate full compliance with a control. Although Audit Manager can provide automated evidence that's helpful and relevant, some automated evidence might only demonstrate partial compliance. In this case, you can supplement the automated evidence that Audit Manager provides with your own evidence.
For example:

- The AWS Generative AI Best Practices Framework v2 contains a control called `Error analysis`. This control requires you to identify when inaccuracies are detected in your model usage. It also requires you to conduct a thorough error analysis to understand the root causes and take corrective action.
- To support this control, Audit Manager collects automated evidence that shows if CloudWatch alarms are enabled for the AWS account where your assessment is running. You can use this evidence to demonstrate partial compliance with the control by proving that your alarms and checks are configured correctly.
- To demonstrate full compliance, you can supplement the automated evidence with manual evidence. For example, you can upload a policy or a procedure that shows your error analysis process, your thresholds for escalations and reporting, and the results of your root cause analysis. You can use this manual evidence to demonstrate that established policies are in place, and that corrective action was taken when prompted.

For a more detailed example, see Controls with mixed data sources.

Export destination

An export destination is the default S3 bucket where Audit Manager saves the files that you export from evidence finder. For more information, see Configuring your default export destination for evidence finder.

F

| B | | | | | G | H | | J | K | L | M | N | O | P | Q | | | T | U | V | W | X | Y | Z

Framework

An Audit Manager framework structures and automate assessments for a specific standard or risk governance principle. These frameworks include a collection of prebuilt or customer defined controls, and they help you to map your AWS resources to the requirements of these controls.

There are two types of framework in Audit Manager.

Framework type	Description
Standard framework	This is a prebuilt framework that is based on AWS best practices for various compliance standards and regulations. You can use standard frameworks to assist with audit preparation for a specific compliance standard or regulation, such as PCI DSS or HIPAA.
Custom framework	This is a customized frameworks that you define as an Audit Manager user. You can use custom frameworks to assist with audit preparation according to your specific GRC requirements.

For instructions on how to create and manage frameworks, see Using the framework library to manage frameworks in AWS Audit Manager.

> **Note**
>
> AWS Audit Manager assists in collecting evidence that's relevant for verifying compliance with specific compliance standards and regulations. However, it doesn't assess your compliance itself. The evidence that's collected through AWS Audit Manager therefore might not include all the information about your AWS usage that's needed for audits. AWS Audit Manager isn't a substitute for legal counsel or compliance experts.

Framework sharing

You can use the Sharing a custom framework in AWS Audit Manager feature to quickly share your custom frameworks across AWS accounts and Regions. To share a custom framework,

you create a *share request.* The recipient then has 120 days to accept or decline the request. When they accept, Audit Manager replicates the shared custom framework into their framework library. In addition to replicating the custom framework, Audit Manager also replicates any custom control sets and controls that are contained within that framework. These custom controls are added to the recipient's control library. Audit Manager doesn't replicate standard frameworks or controls. This is because these resources are already available by default in each account and Region.

I

| B | | | | | G | H | | J | K | L | M | N | O | P | Q | | | T | U | V | W | X | Y | Z

Inconclusive Evidence

AWS Audit Manager marks evidence as inconclusive when automated compliance evaluation isn't possible. This occurs in the following situations:

- You haven't enabled AWS Config or AWS Security Hub, which are key data sources.
- Evidence is collected directly from AWS services via API calls, AWS CloudTrail logs, or manual uploads.

When there's no mechanism for automatic evaluation of this evidence, AWS Audit Manager can't provide evaluation details. As a result, it marks the evidence as *inconclusive*.

> **Important**
>
> Inconclusive evidence doesn't indicate failure. Instead, it signals that you need to manually evaluate the evidence for compliance.

R

| B | | | | | G | H | | J | K | L | M | N | O | P | Q | | | T | U | V | W | X | Y | Z

Resource

A resource is a physical or information asset that's assessed in an audit. Examples of AWS resources include Amazon EC2 instances, Amazon RDS instances, Amazon S3 buckets, and Amazon VPC subnets.

Resource assessment

A resource assessment is the process of assessing an individual resource. This assessment is based on the requirement of a control. While an assessment is active, Audit Manager runs resource assessments for each individual resource in the scope of the assessment. A resource assessment runs the following set of tasks:

1. Collects evidence including resource configurations, event logs, and findings
2. Translates and maps evidence to controls
3. Stores and tracks the lineage of evidence to enable integrity

Resource compliance

Resource compliance refers to the evaluation status of a resource that was assessed when collecting compliance check evidence.

Audit Manager collects compliance check evidence for controls that use AWS Config and Security Hub as a data source type. Multiple resources might be assessed during this evidence collection. As a result, a single piece of compliance check evidence can include one or more resources.

You can use the **Resource compliance** filter in evidence finder to explore compliance status at the resource level. After your search is complete, you can then preview the resources that matched your search query.

In evidence finder, there are three possible values for resource compliance:

Value	Description
Non-compliant	This refers to resources with compliance check issues. This happens if Security Hub reports a *Fail* result for the resource, or if AWS Config reports a *Non-compliant* result.
Compliant	This refers to resources that don't have compliance check issues. This happens if Security Hub reports a *Pass* result for the resource, or if AWS Config reports a *Compliant* result.
Inconclusive	This refers to resources for which a compliance check isn't available or applicable.

Value	Description
	This happens if AWS Config or Security Hub is the underlying data source type, but those services aren't enabled. This also happens if the underlying data source type doesn't support compliance checks (such as manual evidence, AWS API calls, or CloudTrail).

S

| B | | | | | G | H | | J | K | L | M | N | O | P | Q | | | T | U | V | W | X | Y | Z

Service in scope

Audit Manager manages which AWS services are in scope for your assessments. If you have an older assessment, it's possible that you manually specified the services in scope in the past. After June 04, 2024, you can't manually specify or edit services in scope.

A *service in scope* is an AWS service that your assessment collects evidence about. When a service is included in the scope of your assessment, Audit Manager assesses that service's resources. Some example resources include the following:

- An Amazon EC2 instance
- An S3 bucket
- An IAM user or role
- A DynamoDB table
- A network component such as an Amazon Virtual Private Cloud (VPC), security group, or network access control list (ACL) table

For example, if Amazon S3 is a service in scope, Audit Manager can collect evidence about your S3 buckets. The exact evidence that's collected is determined by a control's data source. For instance, if the data source type is AWS Config, and the data source mapping is an AWS Config rule (such as `s3-bucket-public-write-prohibited`), Audit Manager collects the result of that rule evaluation as evidence.

> **Note**
>
> Keep in mind that a service in scope is different to a *data source type*, which can also be an AWS service or something else. For more information, see What's the difference

between a service in scope and a data source type? in the *Troubleshooting* section of this guide.

Standard control

See control.

Understanding how AWS Audit Manager collects evidence

Each active assessment in AWS Audit Manager automatically collects evidence from a range of data sources. In each assessment, you define which AWS accounts Audit Manager will collect evidence for, and Audit Manager manages which AWS services are in scope. Each of these services and accounts contain multiple resources that you own and use. Evidence collection in Audit Manager involves the assessment of each in-scope resource. This is referred to as a *resource assessment*.

The following steps describe how Audit Manager collects evidence for each resource assessment:

1. Assessing a resource from the data source

To start evidence collection, Audit Manager assesses an in-scope resource from a data source. It does this by capturing a configuration snapshot, a related compliance check result, or user activity. It then runs an analysis to determine which control this data supports. The result of the resource assessment is then saved and converted into evidence. For more information about different evidence types, see evidence in the *AWS Audit Manager concepts and terminology* section of this guide.

2. Converting assessment results to evidence

The result of the resource assessment contains both the original data that's captured from that resource, and the metadata that indicates which control the data supports. Audit Manager converts the original data into an auditor-friendly format. The converted data and metadata are then saved as Audit Manager evidence before being attached to a control.

3. Attaching evidence to the related control

Audit Manager reads the evidence metadata. Then, it attaches the saved evidence to a related control within the assessment. The attached evidence becomes visible in Audit Manager. This completes the cycle of a resource assessment.

> **Note**
>
> Depending on the control configurations, the same evidence can, in some cases, be attached to multiple controls from multiple Audit Manager assessments. When the same evidence is attached to multiple controls, Audit Manager meters the resource assessment exactly once. This is because the same evidence is collected exactly only once. However, one control in an Audit Manager assessment can have multiple pieces of evidence from multiple data sources.

Evidence collection frequency

Evidence collection is an ongoing process that starts when you create your assessment. Audit Manager collects evidence from multiple data sources at varying frequencies. As a result, there's no one-size-fits-all answer for how often evidence is collected. The frequency of evidence collection is based on the evidence type and its data source, as described below.

- **Compliance checks** — Audit Manager collects this evidence type from AWS Security Hub and AWS Config.
  - For Security Hub, evidence collection follows the schedule of your Security Hub checks. For more information about the schedule of Security Hub checks, see Schedule for running security checks in the *AWS Security Hub User Guide*. For more information about the Security Hub checks supported by Audit Manager, see AWS Security Hub controls supported by AWS Audit Manager.
  - For AWS Config, evidence collection follows the triggers that are defined in your AWS Config rules. For more information about the triggers for AWS Config rules, see Trigger types in the *AWS Config User Guide*. For more information about the AWS Config Rules that are supported by Audit Manager, see AWS Config Rules supported by AWS Audit Manager.
  - AWS Audit Manager marks evidence as inconclusive when automated compliance evaluation isn't possible. This occurs when you haven't enabled AWS Config or AWS Security Hub, which are key data sources. It also happens when evidence is collected directly from AWS services via API calls, AWS CloudTrail logs, or manual uploads. When there's no mechanism for automatic evaluation of this evidence, AWS Audit Manager can't provide evaluation details. As a result, it marks the evidence as inconclusive. Inconclusive evidence doesn't indicate failure. Instead, it signals that you need to manually evaluate the evidence for compliance.

- **User activity** — Audit Manager collects this evidence type from AWS CloudTrail in a continual manner. This frequency is continual because user activity can happen at any time of the day. For more information, see AWS CloudTrail event names supported by AWS Audit Manager.
- **Configuration data** — Audit Manager collects this evidence type using a describe API call to another AWS service such as Amazon EC2, Amazon S3, or IAM. You can choose which API actions to call. You also set the frequency as daily, weekly, or monthly in Audit Manager. You can specify this frequency when you create or edit a control in the control library. For instructions on how to edit or create a control, see Using the control library to manage controls in AWS Audit Manager. For more information about the API calls that are supported by Audit Manager, see AWS API calls supported by AWS Audit Manager.

Regardless of the evidence collection frequency for the data source, new evidence is collected automatically for as long as the control and the assessment are active.

Examples of AWS Audit Manager controls

You can review the examples on this page to learn more about how controls work in AWS Audit Manager.

In Audit Manager, controls can automatically collect evidence from four data source types:

1. **AWS CloudTrail** – Capture user activity from your CloudTrail logs and import it as user activity evidence
2. **AWS Security Hub** – Collect findings from Security Hub and import them as compliance check evidence
3. **AWS Config** – Collect rule evaluations from AWS Config and import them as compliance check evidence
4. **AWS API calls** – Capture a resource snapshot from an API call and import it as configuration data evidence

Note that some controls collect evidence using predefined groupings of these data sources. These data source groupings are known as AWS managed sources. Each AWS managed source represents either a common control or a core control. These managed sources give you an efficient way to map your compliance requirements to a relevant group of underlying data sources that's validated and maintained by industry certified assessors in AWS.

The examples on this page show how controls collect evidence from each of the individual data source types. They describe what a control looks like, how Audit Manager collects evidence from the data source, and the next steps that you can take to demonstrate compliance.

> **Tip**
>
> We recommend that you enable AWS Config and Security Hub for an optimal experience in Audit Manager. When you enable these services, Audit Manager can use Security Hub findings and AWS Config Rules to generate automated evidence.
>
> - After you enable AWS Security Hub, make sure that you also enable all security standards and turn on the consolidated control findings setting. This step ensures that Audit Manager can import findings for all supported compliance standards.
> - After you enable AWS Config, make sure that you also enable the relevant AWS Config Rules or deploy a conformance pack for the compliance standard that's related to your audit. This step ensures that Audit Manager can import findings for all the supported AWS Config Rules that you enabled.

Examples are available for each of the following types of controls:

Topics

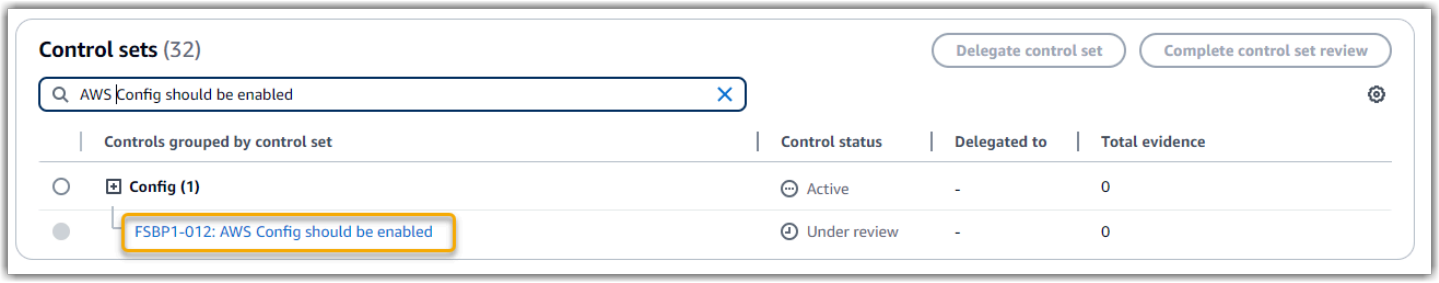
Automated controls that use AWS Security Hub as a data source type

This example shows a control that uses AWS Security Hub as a data source type. This is a standard control taken from the AWS Foundational Security Best Practices (FSBP) framework. Audit Manager uses this control to generate evidence that can help to bring your AWS environment in line with FSBP requirements.

Example control details

- **Control name** – `FSBP1-012: AWS Config should be enabled`
- **Control set** – `Config`. This is a framework-specific grouping of FSBP controls that relate to configuration management.
- **Evidence source** – Individual data sources
- **Data source type** – AWS Security Hub
- **Evidence type** – Compliance check

In the following example, this control appears in an Audit Manager assessment that was created from the FSBP framework.



The assessment shows the control status. It also shows how much evidence was collected for this control so far. From here, you can delegate the control set for review or complete the review yourself. Choosing the control name opens a detail page with more information, including the evidence for that control.

What this control does

This control requires that AWS Config is enabled in all AWS Regions where you use Security Hub. Audit Manager can use this control to check whether you have enabled AWS Config.

How Audit Manager collects evidence for this control

Audit Manager takes the following steps to collect evidence for this control:

1. For each control, Audit Manager assesses your in-scope resources. It does this using the data source that's specified in the control settings. In this example, your AWS Config settings are the resource, and Security Hub is the data source type. Audit Manager looks for the result of a specific Security Hub check ([Config.1]).
2. The result of the resource assessment is saved and converted into auditor-friendly evidence. Audit Manager generates *compliance check* evidence for controls that use Security Hub as a data

source type. This evidence contains the result of the compliance check reported directly from Security Hub.

3. Audit Manager attaches the saved evidence to the control in your assessment that's named `FSBP1-012: AWS Config should be enabled`.

How you can use Audit Manager to demonstrate compliance with this control

After the evidence is attached to the control, you—or a delegate of your choice—can review the evidence to see if any remediation is necessary.

In this example, Audit Manager might display a *Fail* ruling from Security Hub. This can happen if you have not enabled AWS Config. In this case, you can take the corrective action of enabling AWS Config, which helps to bring your AWS environment in line with FSBP requirements.

When your AWS Config settings are in line with the control, mark the control as *Reviewed* and add the evidence to your assessment report. You can then share this report with auditors to demonstrate that the control is working as intended.

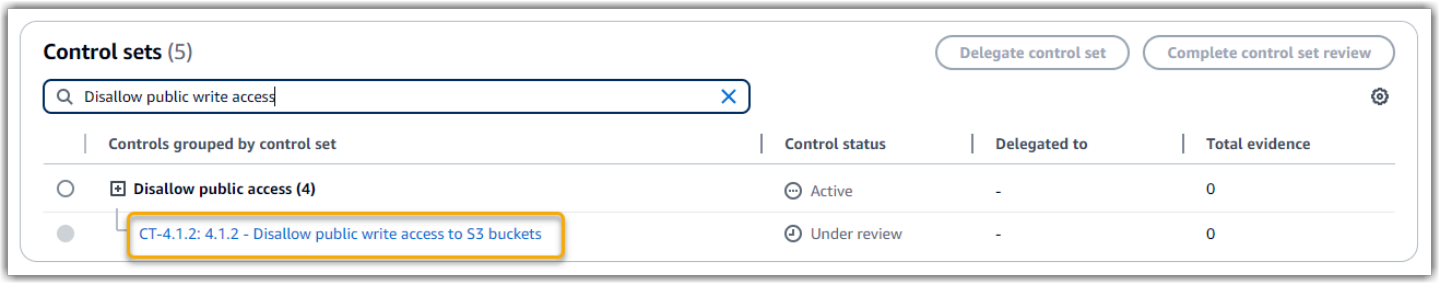
Automated controls that use AWS Config as a data source type

This example shows a control that uses AWS Config as a data source type. This is a standard control taken from the AWS Control Tower Guardrails framework. Audit Manager uses this control to generate evidence that helps bring your AWS environment in line with AWS Control Tower Guardrails.

Example control details

- **Control name** – `CT-4.1.2: 4.1.2 - Disallow public write access to S3 buckets`
- **Control set** – This control belongs to the `Disallow public access` control set. This is a grouping of controls that relate to access management.
- **Evidence source** – Individual data source
- **Data source type** – AWS Config
- **Evidence type** – Compliance check

In the following example, this control appears in an Audit Manager assessment that was created from the AWS Control Tower Guardrails framework.



The assessment shows the control status. It also shows how much evidence was collected for this control so far. From here, you can delegate the control set for review or complete the review yourself. Choosing the control name opens a detail page with more information, including the evidence for that control.

What this control does

Audit Manager can use this control to check if the access levels of your S3 bucket policies are too lenient to meet AWS Control Tower requirements. More specifically, it can check the Block Public Access settings, the bucket policies, and the bucket access control lists (ACL) to confirm that your buckets don't allow public write access.

How Audit Manager collects evidence for this control

Audit Manager takes the following steps to collect evidence for this control:

1. For each control, Audit Manager assesses your in-scope resources using the data source that's specified in the control settings. In this case, your S3 buckets are the resource, and AWS Config is the data source type. Audit Manager looks for the result of a specific AWS Config Rule (s3-bucket-public-write-prohibited) to evaluate the settings, policy, and ACL of each of the S3 buckets that are in scope of your assessment.
2. The result of the resource assessment is saved and converted into auditor-friendly evidence. Audit Manager generates *compliance check* evidence for controls that use AWS Config as a data source type. This evidence contains the result of the compliance check reported directly from AWS Config.
3. Audit Manager attaches the saved evidence to the control in your assessment that's named `CT-4.1.2: 4.1.2 - Disallow public write access to S3 buckets`.

How you can use Audit Manager to demonstrate compliance with this control

After the evidence is attached to the control, you—or a delegate of your choice—can review the evidence to see if any remediation is necessary.

In this example, Audit Manager might display a ruling from AWS Config stating that an S3 bucket is *noncompliant*. This could happen if one of your S3 buckets has a Block Public Access setting that doesn't restrict public policies, and the policy that's in use allows public write access. To remediate this, you can update the Block Public Access setting to restrict public policies. Or, you can use a different bucket policy that doesn't allow public write access. This corrective action helps to bring your AWS environment in line with AWS Control Tower requirements.

When you're satisfied that your S3 bucket access levels are in line with the control, you can mark the control as *Reviewed* and add the evidence to your assessment report. You can then share this report with auditors to demonstrate that the control is working as intended.

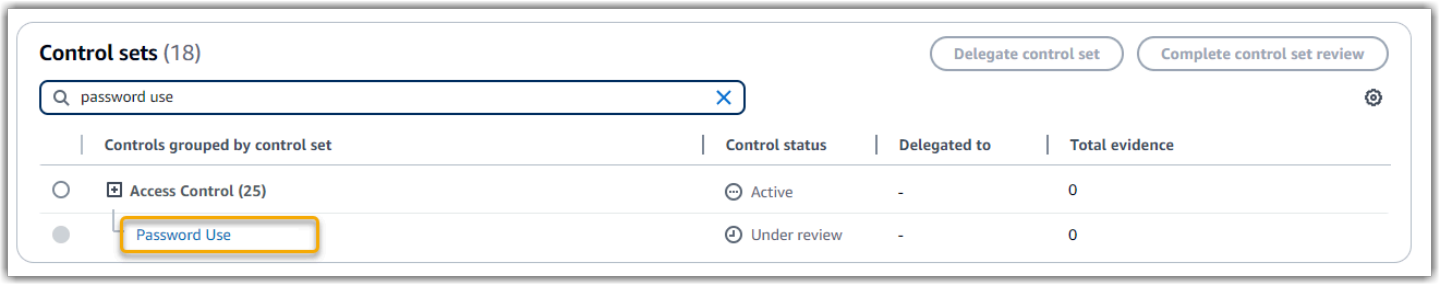
Automated controls that use AWS API calls as a data source type

This example shows a custom control that uses AWS API calls as a data source type. Audit Manager uses this control to generate evidence that can help to bring your AWS environment in line with your specific requirements.

Example control details

- **Control name** – `Password Use`
- **Control set** – This control belongs to a control set that's called `Access Control`. This is a grouping of controls that relate to identity and access management.
- **Evidence source** – Individual data source
- **Data source type** – AWS API calls
- **Evidence type** – Configuration data

In the following example, this control appears in an Audit Manager assessment that was created from a custom framework.



The assessment shows the control status. It also shows how much evidence was collected for this control so far. From here, you can delegate the control set for review or complete the review yourself. Choosing the control name opens a detail page with more information, including the evidence for that control.

What this control does

Audit Manager can use this custom control to help you ensure that you have sufficient access control policies in place. This control requires that you follow good security practices in the selection and use of passwords. Audit Manager can help you to validate this by retrieving a list of all password policies for the IAM principals that are in the scope of your assessment.

How Audit Manager collects evidence for this control

Audit Manager takes the following steps to collect evidence for this custom control:

1. For each control, Audit Manager assesses your in-scope resources using the data source that's specified in the control settings. In this case, your IAM principals are the resources, and AWS API calls is the data source type. Audit Manager looks for the response of a specific IAM API call (GetAccountPasswordPolicy). It then returns the password policies for the AWS accounts that are in scope of your assessment.
2. The result of the resource assessment is saved and converted into auditor-friendly evidence. Audit Manager generates *configuration data* evidence for controls that use API calls as a data source. This evidence contains the original data that's captured from the API responses, and additional metadata that indicates which control the data supports.
3. Audit Manager attaches the saved evidence to the custom control in your assessment that's named `Password Use`.

How you can use Audit Manager to demonstrate compliance with this control

After the evidence is attached to the control, you—or a delegate of your choice—can review the evidence to see if it's sufficient or if any remediation is necessary.

In this example, you can review the evidence to see the response from the API call. The GetAccountPasswordPolicy response describes the complexity requirements and mandatory rotation periods for the user passwords in your account. You can use this API response as evidence to show that you have sufficient password access control policies in place for the AWS accounts that are in the scope of your assessment. If you want, you can also provide additional commentary about these policies by adding a comment to the control.

When you're satisfied that the password policies of your IAM principals are in line with the custom control, you can mark the control as *Reviewed* and add the evidence to your assessment report. You can then share this report with auditors to demonstrate that the control is working as intended.

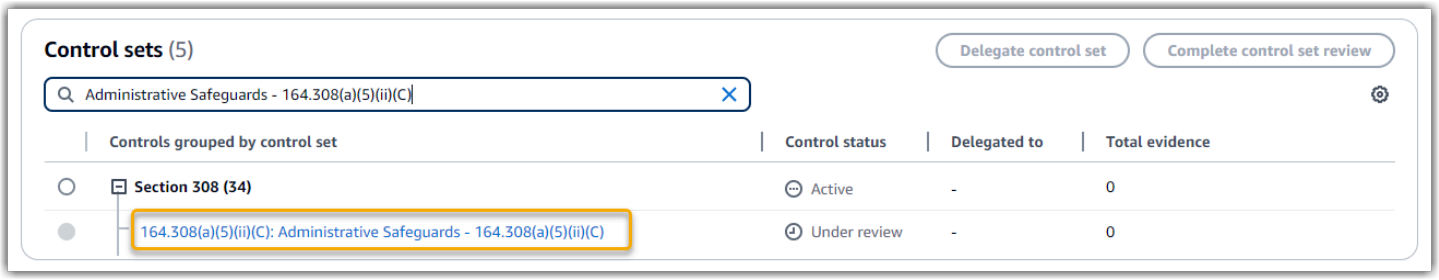
Automated controls that use AWS CloudTrail as a data source type

This example shows a control that uses AWS CloudTrail as a data source type. This is a standard control taken from the HIPAA Security Rule 2003 framework. Audit Manager uses this control to generate evidence that can help to bring your AWS environment in line with HIPAA requirements.

Example control details

- **Control name** – `164.308(a)(5)(ii)(C): Administrative Safeguards - 164.308(a)(5)(ii)(C)`
- **Control set** – This control belongs to the control set that's called `Section 308`. This is a framework-specific grouping of HIPAA controls that relate to administrative safeguards.
- **Evidence source** – AWS managed source (core controls)
- **Underlying data source type** – AWS CloudTrail
- **Evidence type** – User activity

Here's this control shown within an Audit Manager assessment that was created from the HIPAA framework:



The assessment shows the control status. It also shows how much evidence was collected for this control so far. From here, you can delegate the control set for review or complete the review yourself. Choosing the control name opens a detail page with more information, including the evidence for that control.

What this control does

This control requires that you have monitoring procedures in place for detecting unauthorized access. An example of unauthorized access is when someone signs in to the console without multi-

factor authentication (MFA) enabled. Audit Manager helps you to validate this control by providing evidence that you configured Amazon CloudWatch to monitor for management console sign-in requests where MFA is not enabled.

How Audit Manager collects evidence for this control

Audit Manager takes the following steps to collect evidence for this control:

1. For each control, Audit Manager assesses your in-scope resources using the evidence sources that are specified in the control settings. In this case, the control uses several core controls as evidence sources.

   Each core control is a managed grouping of individual data sources. In our example, one of these core controls (`Configure Amazon CloudWatch alarms to detect management console sign-in requests without MFA enabled`) uses a CloudTrail event (`monitoring_EnableAlarmActions`) as the underlying data source.

   Audit Manager reviews your CloudTrail logs, using the `monitoring_EnableAlarmActions` keyword to find CloudWatch alarm enabling actions that are logged by CloudTrail. It then returns a log of the relevant events that are within the scope of your assessment.
2. The result of the resource assessment is saved and converted into auditor-friendly evidence. Audit Manager generates *user activity* evidence for controls that use CloudTrail as a data source type. This evidence contains the original data that's captured from Amazon CloudWatch, and additional metadata that indicates which control the data supports.
3. Audit Manager attaches the saved evidence to the control in your assessment that's named `164.308(a)(5)(ii)(C): Administrative Safeguards - 164.308(a)(5)(ii)(C)`.

How you can use Audit Manager to demonstrate compliance with this control

After the evidence is attached to the control, you—or a delegate of your choice—can review the evidence to see if any remediation is necessary.

In this example, you can review the evidence to see the alarm enablement events that were logged by CloudTrail. You can use this log as evidence to show that you have sufficient monitoring procedures in place to detect when console sign-ins occur without MFA enabled. If you like, you can also provide additional commentary by adding a comment to the control. For example, if the log shows multiple sign-ins without MFA, you can add a comment that describes how you remediated the issue. Regular monitoring of console sign-ins helps you to prevent security problems that may

arise from discrepancies and inappropriate sign-in attempts. In turn, this best practice helps to bring your AWS environment in line with HIPAA requirements.

When you're satisfied that your monitoring procedure is in line with the control, you can mark the control as *Reviewed* and add the evidence to your assessment report. You can then share this report with auditors to demonstrate that the control is working as intended.

Manual controls

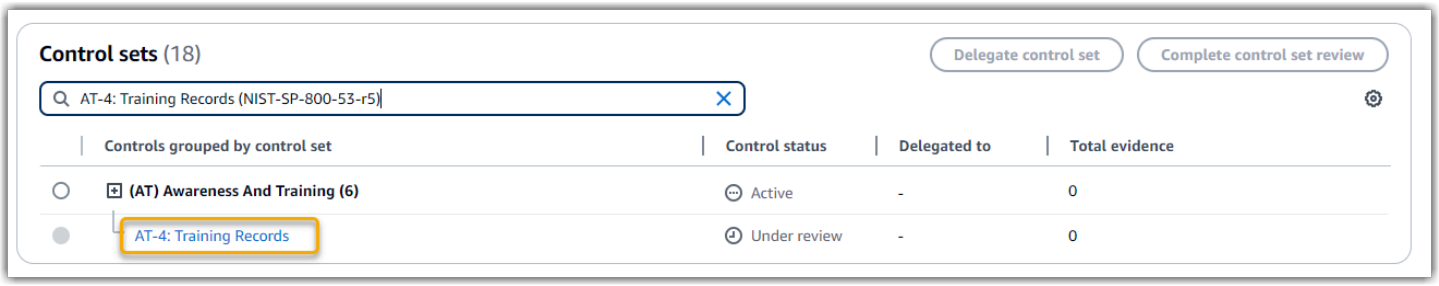
Some controls don't support automated evidence collection. This includes controls that rely on the provision of physical records and signatures, in addition to observations, interviews, and other events that aren't generated in the cloud. In these cases, you can manually upload evidence to demonstrate that you're satisfying the requirements of the control.

This example shows a manual control taken from the NIST 800-53 (Rev. 5) framework. You can use Audit Manager to upload and store evidence that demonstrates compliance for this control.

Example control details

- **Control name** – `AT-4: Training Records`
- **Control set** – `(AT) Awareness and training`. This is a framework-specific grouping of NIST controls that relate to training.
- **Evidence source** – Individual data source
- **Data source type** – Manual
- **Evidence type** – Manual

Here's this control shown within an Audit Manager assessment that was created from the NIST 800-53 (Rev. 5) Low-Moderate-High framework:



The assessment shows the control status. It also shows how much evidence was collected for this control so far. From here, you can delegate the control set for review or complete the review

yourself. Choosing the control name opens a detail page with more information, including the evidence for that control.

What this control does

You can use this control to help you ensure that your personnel receive the appropriate level of security and privacy training. Specifically, you can demonstrate that you have documented security and privacy training activities in place for all staff, based on their role. You can also show proof that training records are retained for each individual.

How you can manually upload evidence for this control

To upload manual evidence that supplements the automated evidence, see Uploading manual evidence in AWS Audit Manager. Audit Manager attaches the uploaded evidence to the control in your assessment that's named `AT-4: Training Records`.

How you can use Audit Manager to demonstrate compliance with this control

If you have documentation that supports this control, you can upload it as manual evidence. For example, you can upload the latest copy of mandated role-based training materials that your Human Resources department issues to employees.

Much like with automated controls, you can delegate manual controls to stakeholders who can help you to review evidence (or, in this case, supply it). For example, when you review this control, you might realize that you only partially meet its requirements. This could be the case if you don't have a copy of any attendance tracking for in-person trainings. You could delegate the control to an HR stakeholder, who can then upload a list of staff that attended the training.

When you're satisfied that you're in line with the control, you can mark it as *Reviewed* and add the evidence to your assessment report. You can then share this report with auditors to demonstrate that the control is working as intended.

Controls with mixed data source types (automated and manual)

In many cases, a combination of automated and manual evidence is needed to satisfy a control. Although Audit Manager can provide automated evidence that's relevant to the control, you might need to supplement this data with manual evidence that you identify and upload yourself.

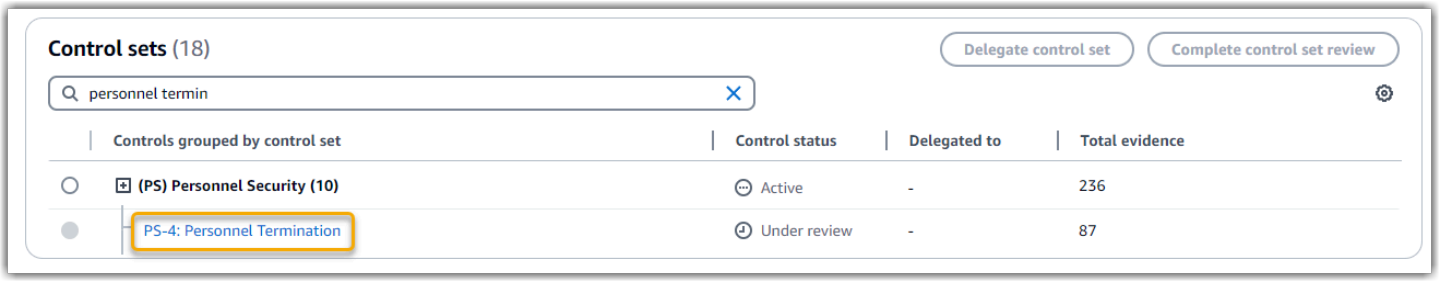
This example shows a control that uses a combination of manual evidence and automated evidence. This is a standard control taken from the NIST 800-53 (Rev. 5) framework. Audit Manager

uses this control to generate evidence that can help to bring your AWS environment in line with NIST requirements.

Example control details

- **Control name** – `Personnel Termination`
- **Control set** – `(PS) Personnel Security (10)`. This is a framework-specific grouping of NIST controls that relate to the individuals who perform hardware or software maintenance on organizational systems.
- **Evidence source** – AWS managed (core controls) and individual data sources (manual)
- **Underlying data source type** – AWS API calls, AWS CloudTrail, AWS Config, Manual
- **Evidence type** – Configuration data, user activity, compliance check, manual evidence)

Here's this control shown within an Audit Manager assessment that was created from the NIST 800-53 (Rev. 5) framework:



The assessment shows the control status. It also shows how much evidence was collected for this control so far. From here, you can delegate the control set for review or complete the review yourself. Choosing the control name opens a detail page with more information, including the evidence for that control.

What this control does

You can use this control to confirm that you're protecting organizational information in the event that an employee is terminated. Specifically, you can demonstrate that you disabled system access and revoked credentials for the individual. Moreover, you can demonstrate that all terminated individuals participated in an exit interview that included discussion of the relevant security protocols for your organization.

How Audit Manager collects evidence for this control

Audit Manager takes the following steps to collect evidence for this control:

1. For each control, Audit Manager assesses your in-scope resources using the evidence sources that are specified in the control settings.

   In this case, the control uses several core controls as evidence sources. In turn, each of these core controls collect relevant evidence from individual data sources (AWS API calls, AWS CloudTrail, and AWS Config). Audit Manager uses these data source types to assess your IAM resources (such as groups, keys, and policies) against the relevant API calls, CloudTrail events, and AWS Config rules.
2. The result of the resource assessment is saved and converted into auditor-friendly evidence. This evidence contains the original data that's captured from each data source, and additional metadata that indicates which control the data supports.
3. Audit Manager attaches the saved evidence to the control in your assessment that's named `Personnel Termination`.

How you can manually upload evidence for this control

To upload manual evidence that supplements the automated evidence, see Uploading manual evidence in AWS Audit Manager. Audit Manager attaches the uploaded evidence to the control in your assessment that's named `Personnel Termination`.

How you can use Audit Manager to demonstrate compliance with this control

After the evidence is attached to the control, you—or a delegate of your choice—can review the evidence to see if it's sufficient or if any remediation is necessary. For example, when you review this control, you might realize that you only partially meet its requirements. This could be the case if you have proof that access was revoked, but don't have a copy of any exit interviews. You could delegate the control to an HR stakeholder, who can then upload a copy of the exit interview paperwork. Or, if no employees were terminated during the audit period, you can leave a comment that states why no signed paperwork is attached to the control.

When you're satisfied that you're in line with the control, mark the control as *Reviewed* and add the evidence to your assessment report. You can then share this report with auditors to demonstrate that the control is working as intended.

Using AWS Audit Manager

You can access AWS Audit Manager through various options, depending on your specific needs and preferences. Here are some different ways you can interact with Audit Manager:

- **Audit Manager console**

  Access the Audit Manager console directly at https://console.aws.amazon.com/auditmanager/home, which provides a user-friendly interface for managing your audits and related resources.

- **Audit Manager API**

  Interact with Audit Manager programmatically through the Audit Manager API, allowing you to automate and integrate tasks into your existing workflows. For more information, see the *AWS Audit Manager API Reference*.

- **AWS SDKs**

  Use AWS software development kits (SDKs) to interact with Audit Manager programmatically, enabling you to write code in various programming languages. For more information, see Using AWS Audit Manager with an AWS SDK.

- **AWS CloudFormation**

  Create Audit Manager resources using AWS CloudFormation, which allows you to define and deploy your auditing infrastructure as code. For more information, see Creating AWS Audit Manager resources with AWS CloudFormation.

- **Third-party integrations**

  Integrate Audit Manager with supported third-party Governance, Risk, and Compliance (GRC) products, enabling you to leverage existing GRC tools and processes. For more information, see Integrations with third-party GRC products.

- **Integrations with your own GRC system**

  Incorporate Audit Manager evidence into your own GRC system, allowing you to send evidence directly from Audit Manager into your GRC application. For more information, see Integrating Audit Manager evidence into your GRC system.

Using AWS Audit Manager with an AWS SDK

AWS software development kits (SDKs) are available for many popular programming languages. Each SDK provides an API, code examples, and documentation that developers can use to build applications in their preferred language.

SDK documentation	Audit Manager specific documentation	Code examples	
AWS SDK for C++	AWS SDK for C++ API reference for Audit Manager	AWS SDK for C++ code examples	
AWS SDK for Go	AWS SDK for Go API reference for Audit Manager	AWS SDK for Go code examples	
AWS SDK for Java	AWS SDK for Java 2.x API reference for Audit Manager	AWS SDK for Java code examples	
AWS SDK for JavaScript	AWS SDK for JavaScript API reference for Audit Manager	AWS SDK for JavaScript code examples	
AWS SDK for .NET	AWS SDK for .NET API reference for Audit Manager	AWS SDK for .NET code examples	
AWS SDK for PHP	AWS SDK for PHP API reference for Audit Manager	AWS SDK for PHP code examples	
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto) API reference for Audit Manager	AWS SDK for Python (Boto3) code examples	
AWS SDK for Ruby	AWS SDK for Ruby API reference for Audit Manager	AWS SDK for Ruby code examples	

For examples that are specific to Audit Manager, see Code examples for Audit Manager using AWS SDKs.

Note

Audit Manager is available in botocore version 1.19.32 and later for the AWS SDK for Python (Boto3). Before you start using the SDK, make sure that you're using the appropriate botocore version.

Creating AWS Audit Manager resources with AWS CloudFormation

AWS Audit Manager is integrated with AWS CloudFormation, a service that helps you to model and set up your AWS resources so that you can spend less time creating and managing your resources and infrastructure. You create a template that describes all the AWS resources that you want (such as assessments), and AWS CloudFormation provisions and configures those resources for you.

When you use AWS CloudFormation, you can reuse your template to set up your AWS Audit Manager resources consistently and repeatedly. Describe your resources once, and then provision the same resources over and over in multiple AWS accounts and Regions.

AWS Audit Manager and AWS CloudFormation templates

To provision and configure resources for AWS Audit Manager and related services, you must understand AWS CloudFormation templates. Templates are formatted text files in JSON or YAML. These templates describe the resources that you want to provision in your AWS CloudFormation stacks. If you're unfamiliar with JSON or YAML, you can use AWS CloudFormation Designer to help you get started with AWS CloudFormation templates. For more information, see What is AWS CloudFormation Designer? in the *AWS CloudFormation User Guide*.

AWS Audit Manager supports creating assessments in AWS CloudFormation. For more information, including examples of JSON and YAML templates for assessments, see the AWS Audit Manager resource type reference in the *AWS CloudFormation User Guide*.

Learn more about AWS CloudFormation

To learn more about AWS CloudFormation, see the following resources:

- AWS CloudFormation
- AWS CloudFormation User Guide
- AWS CloudFormation API Reference
- AWS CloudFormation Command Line Interface User Guide

Integrations with third-party GRC products

AWS Audit Manager supports integrations with the third-party partner GRC products that are listed on this page.

If your company uses a hybrid cloud model or multicloud model, it's likely that you use a GRC product to manage evidence from those environments. When that product is integrated with Audit Manager, you can pull evidence about your AWS usage directly into your GRC environment. This simplifies how you manage compliance by providing you with a centralized place to review and remediate evidence as you prepare for audits.

Read this page for an overview of the third-party GRC products that can ingest evidence from Audit Manager. You can also see a reference of which Audit Manager API actions you can take directly within those products.

Topics

Understanding how third-party integrations work with Audit Manager

GRC partners can use the Audit Manager public APIs to integrate their products with Audit Manager. With this integration in place, you can map the enterprise controls in your GRC environment to the common controls that Audit Manager provides.

> **Tip**
>
> You can map your enterprise controls to any type of Audit Manager control. However, we recommend that you use common controls. When you map to a common control that represents your goal, Audit Manager collects evidence from a predefined group of data sources that's managed by AWS. This means that you don't have to be an AWS expert to know which data sources collect the relevant evidence for your goal.

After you complete this one-time control mapping exercise, you can create Audit Manager assessments directly in the GRC product. This action starts the collection of evidence about your AWS usage. You can then see this AWS evidence along with the other evidence that's collected from your hybrid environment, all within the same context of your enterprise controls.

When you use an Audit Manager integration with a third-party GRC product, keep in mind the following points:

- Integrations are available for all AWS Regions where Audit Manager is supported.

- Any Audit Manager resources that you create in the GRC partner product are also reflected in Audit Manager.
- You're subject to AWS Audit Manager pricing in addition to the pricing of the third-party GRC product.
- The evidence that Audit Manager collects is immutable. Evidence is presented in exactly the same way in third-party GRC products as it is in the Audit Manager console. However, if you use a third-party integration, you might be able to enhance this evidence by providing additional context in your reporting.
- The same quotas that apply to Audit Manager also apply within the third-party GRC product. For example, each AWS account can have up to 100 active Audit Manager assessments. This account-level quota applies whether you create the assessments in the Audit Manager console or in the third-party GRC product. Most Audit Manager quotas, but not all, are listed under the AWS Audit Manager namespace in the Service Quotas console. To learn how to request a quota increase, see Managing your Audit Manager quotas.

If you have a compliance solution and you're interested in integrating with Audit Manager, email `auditmanager-partners@amazon.com`.

Third-party GRC partner products that integrate with Audit Manager

The following third party GRC products can ingest evidence from Audit Manager.

MetricStream

To use this integration, reach out to MetricStream for the access and purchase of MetricStream GRC software.

Built on the MetricStream Platform, the MetricStream Enterprise GRC solution allows for a comprehensive and collaborative approach to enterprise-wide GRC activities and processes. By ingesting evidence from Audit Manager into MetricStream, you can proactively identify non-compliant evidence from your AWS environment and review it alongside evidence from your on-premises data sources or other cloud partners. This provides you with a convenient and centralized way to review and improve your cloud security and compliance posture as you prepare for audits.

With the MetricStream and Audit Manager integration, you can perform the following API operations.

Task	API operation
Setting up the Audit Manager integration	• GetAccountStatus • GetOrganizationAdminAccount • GetSettings
Reviewing Audit Manager resources	• GetAssessment • GetAssessmentFramework • GetControl • ListAssessmentFrameworks • ListControls
Creating Audit Manager resources	• CreateAssessment • CreateAssessmentFramework
Updating Audit Manager resources	• UpdateAssessment • UpdateAssessmentControl • UpdateAssessmentStatus
Managing evidence	• StartQuery (AWS CloudTrail API) • GetQueryResults (AWS CloudTrail API)
Deleting Audit Manager resources	• DeleteAssessmentFramework

Related MetricStream links

- AWS Marketplace link
- Product link
- Product pricing

Integrating Audit Manager evidence into your GRC system

As an enterprise customer, you likely have resources across multiple data centers, including other cloud vendors and on-premises environments. To collect evidence from these environments, you might use third-party GRC (Governance, Risk, and Compliance) solutions such as MetricStream CyberGRC or RSA Archer. Or, you might use a proprietary GRC system that you developed in-house.

This tutorial shows you how you can integrate your internal or external GRC system with Audit Manager. This integration enables vendors to collect evidence about their customers' AWS usage and configurations, and send that evidence directly from Audit Manager into the GRC application. By doing this, you can centralize your compliance reporting across multiple environments.

For the purpose of this tutorial:

1. A **vendor** is the entity or company who owns the GRC application that's being integrated with Audit Manager.
2. A **customer** is the entity or company who uses AWS, and who also uses an internal or external GRC application.

> **Note**
>
> In some cases, the GRC application is owned and used by same company. In this scenario, the **vendor** is the group or team who owns the GRC application, and the **customer** is the team or group that uses the GRC application.

This tutorial shows you how to do the following:

- Step 1: Enable Audit Manager
- Step 2: Set up permissions
- Step 3. Map your enterprise controls to Audit Manager controls
- Step 4. Keep your control mappings updated
- Step 5: Create an assessment
- Step 6. Start collecting evidence

Prerequisites

Before you get started, make sure that you meet the following conditions:

- You have an infrastructure running in AWS.
- You use an in-house GRC system, or you use third-party GRC software that's provided by a vendor.
- You completed all the prerequisites that are needed to set up Audit Manager.
- You're familiar with Understanding AWS Audit Manager concepts and terminology.

Some restrictions to keep in mind:

- Audit Manager is a Regional AWS service. You must set up Audit Manager separately in each Region where you run your AWS workloads.
- Audit Manager doesn't support the aggregation of evidence from multiple Regions into a single Region. If your resources span across multiple AWS Regions, you must aggregate the evidence within your GRC system.
- Audit Manager has default quotas for the number of resources you can create. You can request an increase to these default quotas if needed. For more information, see Quotas and restrictions for AWS Audit Manager.

Step 1: Enable Audit Manager

Who completes this step

Customer

What you need to do

Start by enabling Audit Manager for your AWS account. If your account is part of an organization, you can enable Audit Manager using your management account and then specify a delegated administrator for Audit Manager.

Procedure

To enable Audit Manager

Follow the instructions to Enable Audit Manager. Repeat the setup procedure for all Regions where you want to collect evidence.

Tip

If you use AWS Organizations, we strongly recommend that you set up a delegated administrator during this step. When you use a delegated administrator account in Audit Manager, you can use evidence finder to search for evidence across all member accounts in your organization.

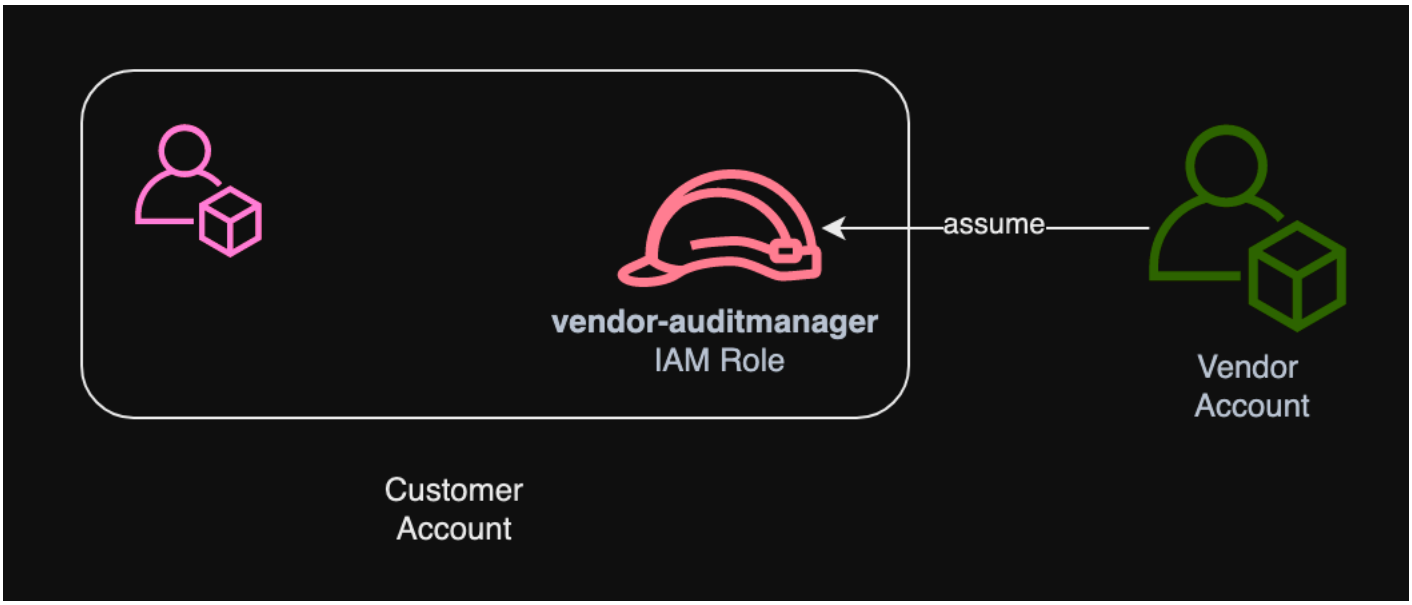
Step 2: Set up permissions

Who completes this step

Customer

What you need to do

In this step, the customer creates an IAM role for their account. The customer then gives the vendor permissions to assume the role.



Procedure

To create a role for the customer account

Follow the instructions in Creating a role for an IAM user in the *IAM User Guide.*

- In step 8 of the role creation workflow, choose **Create policy** and enter a policy for the role.

At minimum, the role must have the following permissions:

JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AuditManagerAccess",
      "Effect" : "Allow",
      "Action" : [
        "auditmanager:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListChildren"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser",
        "iam:ListUsers",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3Access",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsCreateGrantAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "auditmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SNSAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagAccess",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

- In step 11 of the role creation workflow, enter `vendor-auditmanager` as the **Role name**.

To allow the vendor account to assume the role

Follow the instructions in Granting users permission to switch roles in the *IAM User Guide*.

- The policy statement must include the `Allow` effect on the `sts:AssumeRole action`.
- It must also include the Amazon Resource Name (ARN) of the role in a Resource element.
- Here is an example policy statement you can use.

  In this policy, replace the *`placeholder text`* with your vendor's AWS account ID.

  JSON

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "sts:AssumeRole",
        "Resource": "arn:aws:iam::111122223333:role/vendor-auditmanager"
    }
}
```

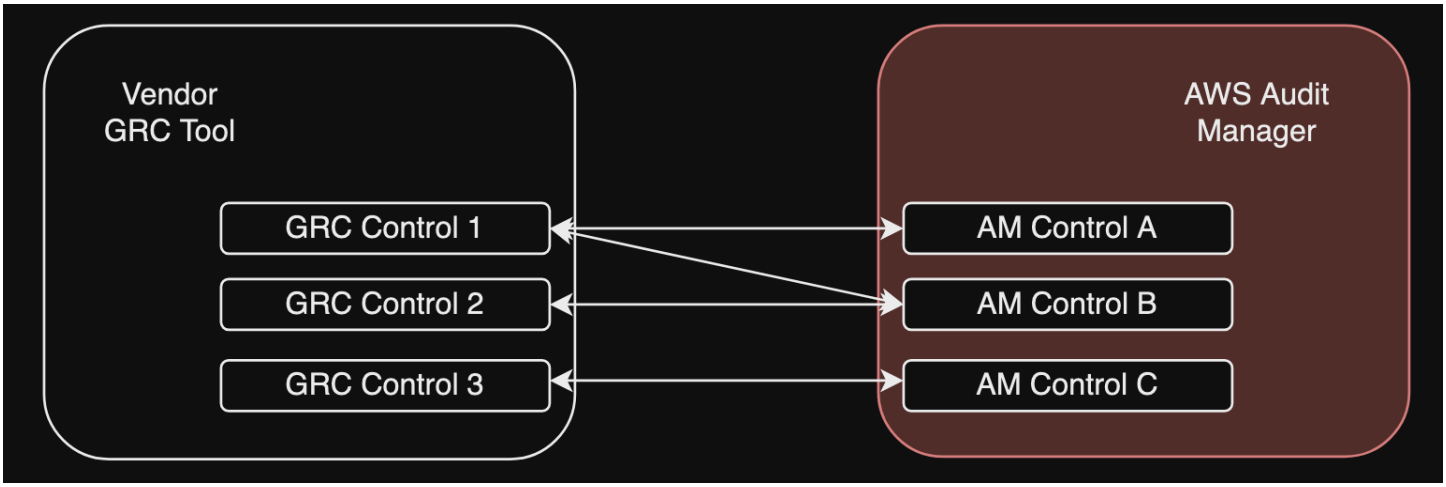
Step 3. Map your enterprise controls to Audit Manager controls

Who completes this step

Customer

What you need to do

Vendors maintain a curated list of enterprise controls that customers can use in an assessment. To integrate with Audit Manager, vendors must create an interface that enables customers to map their enterprise controls to the corresponding Audit Manager controls. You can map to common controls (preferred), or standard controls. You must complete this mapping before you start any assessments in the vendor's GRC application.



Option 1: Map enterprise controls to common controls (recommended)

This is the recommended way to map your enterprise controls to Audit Manager. This is because common controls closely align with common industry standards. This makes it easier to map them to your enterprise controls.

With this approach, the vendor creates an interface that enables the customer to perform a one-time mapping between their enterprise controls and the corresponding common controls that Audit Manager provides. Vendors can use the ListControls, ListCommonControls, and GetControl API operations to surface this information to customers. After the customer completes the mapping exercise, the vendor can then use these mappings to create custom controls in Audit Manager.

Here is an example of a common control mapping:

Let's say that you have an enterprise control named `Asset Management`. This enterprise control maps to two common controls in Audit Manager (`Asset performance management` and `Asset maintenance scheduling`). In this case, you must create a custom control in Audit Manager (we'll name it `enterprise-asset-management`). Then, and add `Asset performance management` and `Asset maintenance scheduling` as evidence sources to the new custom control. These evidence sources collect supporting evidence from a predefined group of AWS data sources. This provides you with an efficient way to identify the AWS data sources that map to the requirements of your enterprise control.

Procedure

To find the available common controls that you can map to

Follow the steps to find the list of available common controls in Audit Manager.

To create a custom control

1. Follow the steps to create a custom control that aligns with your enterprise control.

   When you specify evidence sources in step 2 of the custom control creation workflow, do the following:

   - Choose **AWS managed sources** as the evidence source.
   - Select **Use a common control that matches your compliance goal**.
   - Choose up to five common controls as evidence sources for your enterprise control.
2. Repeat this task for all of your enterprise controls, and create corresponding custom controls in Audit Manager for each one.

Option 2: Map enterprise controls to standard controls

Audit Manager provides a large number of prebuilt standard controls. You can perform a one-time mapping between your enterprise controls and these standard controls. After you've identified the standard controls that correspond to your enterprise controls, you can add these standard controls directly to a custom framework. If you choose this option, you don't need to create any custom controls in Audit Manager.

Procedure

To find the available standard controls that you can map to

Follow the steps to find the list of available standard controls in Audit Manager.

To create a custom framework

1. Follow the steps to create a custom framework in Audit Manager.

   When you specify a control set in step 2 of the framework creation procedure, include the standard controls that map to your enterprise controls.
2. Repeat this task for all of your enterprise controls until you have included all of the corresponding standard controls in your custom framework.

Step 4. Keep your control mappings updated

Who completes this step

Vendor, customer

What you need to do

Audit Manager continuously updates common controls and standard controls to ensure that they use the latest available AWS data sources. This means that mapping controls is a one-off task: you don't need to manage standard controls after you add them to a custom framework, and you don't need to manage common controls after you add them as an evidence source in your custom control. Whenever a common control is updated, the same updates are automatically applied to all custom controls that use that common control as an evidence source.

However, over time it's possible that new common controls and standard controls will become available for you to use as evidence sources. With this in mind, vendors and customers should create a workflow to periodically fetch the latest common controls and standard controls from Audit Manager. You can then review the mappings between the enterprise controls and Audit Manager controls, and update the mappings as needed.

If your enterprise controls are mapped to common controls

During the mapping process, you created custom controls. You can use Audit Manager to edit those custom controls so that they use the latest available common controls as evidence sources. After the custom control updates take effect, your existing assessments will automatically collect evidence against the updated custom controls. There's no need to create a new framework or assessment.

Procedure

To find the latest common controls that you can map to

Follow the steps to find the available common controls in Audit Manager.

To edit a custom control

1. Follow the steps to edit a custom control in Audit Manager.

   When you update the evidence sources in step 2 of the editing workflow, do the following:

   - Choose **AWS managed sources** as the evidence source.

- Select **Use a common control that matches your compliance goal**.
- Choose the new common control that you want to use as an evidence source for your custom control.

2. Repeat this task for all of your enterprise controls that you want to update.

If your enterprise controls are mapped to standard controls

In this case, vendors must create a new custom framework that includes the latest available standard controls, and then create a new assessment using this new framework. After creating the new assessment, you can mark your old assessment as inactive.

Procedure

To find the latest standard controls that you can map to

Follow the steps to find the available standard controls in Audit Manager.

To create a custom framework and add the latest standard controls

Follow the steps to create a custom framework in Audit Manager.

When you specify a control set in step 2 of the framework creation workflow, include the new standard controls.

To create an assessment

Create an assessment in the GRC application.

To change the status of an assessment to inactive

Follow the steps to change the status of an assessment in Audit Manager.

Step 5: Create an assessment

Who completes this step

GRC application, with input from the vendor

What you need to do

As a customer, you don't need to create an assessment directly in Audit Manager. When you start an assessment for certain controls in the GRC application, the GRC application creates

the corresponding resources for you in Audit Manager. Firstly, the GRC application uses the mappings that you created to identify the relevant Audit Manager controls. Next, it uses the control information to create a custom framework for you. Lastly, it uses the newly-created custom framework to create an assessment in Audit Manager.

Creating an assessment in Audit Manager also requires a scope. This scope takes a list of the AWS accounts where the customer wants to run the assessment and collect evidence. Customers must define this scope directly in the GRC application.

As a vendor, you need to store the `assessmentId` that's mapped to the assessment that was started in the GRC application. This `assessmentId` is required to fetch evidence from Audit Manager.

To find an assessment ID

1. Use the ListAssessments operation to view your assessments in Audit Manager. You can use the status parameter to view assessments that are active.

   ```
   aws auditmanager list-assessments --status ACTIVE
   ```

2. In the response, identify the assessment that you want to store in the GRC application, and take note of the `assessmentId`.

Step 6. Start collecting evidence

Who completes this step

AWS Audit Manager, with input from the vendor

What you need to do

After you create an assessment, it takes up to 24 hours to start collecting evidence. At this point, your enterprise controls are now actively collecting evidence for your Audit Manager assessment.

We recommend that you use the evidence finder feature to quickly query and find evidence in Audit Manager. If you use evidence finder as a delegated administrator, you can search for evidence across all member accounts in your organization. Using a combination of filters and groupings, you can progressively narrow the scope of your search query. For example, if you want a high-level view of your system health, perform a broad search and filter by assessment, date range, and resource compliance. If your goal is to remediate a specific resource, you can perform a narrow search to

target evidence for a specific control or resource ID. After you define your filters, you can group and then preview the matching search results before creating an assessment report.

To enable evidence finder

- Follow the instructions to enable evidence finder from your Audit Manager settings.

After you enable evidence finder, you can decide on a cadence to fetch evidence from Audit Manager for your assessment. You can also fetch evidence for a specific control in an assessment, and store the evidence in the GRC application that's mapped to the enterprise control. You can use the following Audit Manager API operations to fetch evidence:

- GetEvidence
- GetEvidenceByEvidenceFolder
- GetEvidenceFolder
- GetEvidenceFoldersByAssessment
- GetEvidenceFoldersByAssessmentControl

Pricing

You won't incur any additional cost for this integration setup, whether you're a vendor or a customer. Customers are charged for the evidence that's collected in Audit Manager. For more information about pricing, see AWS Audit Manager Pricing.

Additional resources

You can learn more about the concepts that are introduced in this tutorial by reviewing the following resources:

- Assessments – Learn about the concepts and tasks for managing an assessment.
- Control library – Learn about the concepts and tasks for managing a custom control.
- Framework library – Learn about the concepts and tasks for managing a custom framework.
- Evidence finder - Learn how to export a CSV file or generate an assessment report from your query results.
- Download center - Learn how to download assessment reports and CSV exports from Audit Manager.

Supported frameworks in AWS Audit Manager

When you explore the framework library in AWS Audit Manager, you'll find a comprehensive list of pre-built standard frameworks that can help you to streamline your compliance efforts. These prebuilt frameworks are based on AWS best practices for various compliance standards and regulations. You can use these frameworks to assist you with your audit preparation, whether you need to assess your environment against HIPAA, PCI DSS, SOC 2, or more.

> **Note**
>
> If you're new to Audit Manager, start with the AWS Audit Manager Sample Framework. This framework is designed for learning purposes and doesn't support any specific compliance standard. It provides a controlled environment for you to explore Audit Manager's core functionality within a manageable scope. After you use the sample framework to familiarize yourself with Audit Manager, you'll be ready to use the other frameworks for actual compliance assessments.

The following list provides an overview of the available frameworks so that you can easily identify the ones that align with your specific requirements. Take a moment to review the list and familiarize yourself with the frameworks that are most relevant to your organization's needs. Open any page to see an overview of that framework and learn how you can use it to create an assessment and start collecting evidence in Audit Manager.

Topics

- AWS Well Architected Framework WAF v10
- CCCS Medium Cloud Control
- CIS AWS Benchmark v1.2.0
- CIS AWS Benchmark v1.3.0
- CIS AWS Benchmark v1.4.0
- CIS Controls v7.1, IG1
- CIS Critical Security Controls version 8.0, IG1
- FedRAMP Security Baseline Controls r4
- GDPR 2016
- Gramm-Leach-Bliley Act
- Title 21 CFR Part 11
- EU GMP Annex 11, v1
- HIPAA Security Rule: Feb 2003
- HIPAA Omnibus Final Rule
- ISO/IEC 27001:2013 Annex A
- NIST SP 800-53 Rev 5
- NIST Cybersecurity Framework v1.1
- NIST SP 800-171 Rev 2
- PCI DSS V3.2.1
- PCI DSS V4.0
- SSAE-18 SOC 2

ACSC Essential Eight

AWS Audit Manager provides a prebuilt standard framework that supports the Australian Cyber Security Center (ACSC) Essential Eight.

Topics

- What is the ACSC Essential Eight?

What is the ACSC Essential Eight?

The ACSC is the Australian government's lead agency for cyber security. To protect against cyber threats, the ACSC recommends that organizations implement eight essential mitigation strategies from the ACSC's *Strategies to Mitigate Cyber Security Incidents* as a baseline. This baseline, known as the Essential Eight, makes it much harder for adversaries to compromise systems.

As the Essential Eight outlines a minimum set of preventative measures, your organization needs to implement additional measures where it is warranted by your environment. Further, while the Essential Eight can help to mitigate the majority of cyber threats, it will not mitigate all cyber threats. As such, additional mitigation strategies and security controls need to be considered, including those from the *Strategies to Mitigate Cyber Security Incidents* and the *Information Security Manual* (ISM).

Using this framework

You can use the Essential Eight standard framework in AWS Audit Manager to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to Essential Eight requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the Essential Eight framework. When it's time for an audit, you—or a delegate of your choice—can review the evidence that Audit Manager collected. Either, you can browse the evidence folders in your assessment and choose which evidence you want to include in your assessment report. Or, if you enabled evidence finder, you can search for specific evidence and export it in CSV format,

or create an assessment report from your search results. Either way, you can use this assessment report to show that your controls are working as intended.

The framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets
Australian Cyber Security Center (ACSC) Essential Eight	61	132	3

Important

To ensure that this framework collects the intended evidence from AWS Security Hub, make sure that you enabled all standards in Security Hub.
To ensure that this framework collects the intended evidence from AWS Config, make sure that you enable the necessary AWS Config rules. To review the AWS Config rules that are used as data source mappings in this standard framework, download the AuditManager_ConfigDataSourceMappings_Australian-Cyber-Security-Center-(ACSC)-Essential-Eight.zip file.

The controls in this AWS Audit Manager framework aren't intended to verify if your systems are compliant with the Essential Eight controls. Moreover, they can't guarantee that you'll pass an ACSC audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

Next steps

For instructions on how to view detailed information about this framework, including the list of standard controls that it contains, see Reviewing a framework in AWS Audit Manager.

For instructions on how to create an assessment using this framework, see Creating an assessment in AWS Audit Manager.

For instructions on how to customize this framework to support your specific requirements, see Making an editable copy of an existing framework in AWS Audit Manager.

Additional resources

- ACSC Essential Eight

ACSC ISM 02 March 2023

AWS Audit Manager provides a prebuilt standard framework that supports the Australian Cyber Security Center (ACSC) Information Security Manual (ISM).

Topics

What is the ACSC ISM?

The ACSC is the Australian government's lead agency for cyber security. The ACSC produces the ISM, which functions as a set of cyber security principles. The purpose of these principles is to provide strategic guidance on how an organization can protect their systems and data from cyber threats. These cyber security principles are grouped into four key activities: govern, protect, detect and respond. An organization should be able to demonstrate that the cyber security principles are being adhered to within their organization. The ISM is intended for Chief Information Security Officers, Chief Information Officers, cyber security professionals, and information technology managers.

Using this framework

You can use the ACSC ISM standard framework in AWS Audit Manager to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing

procedures. These controls are grouped into control sets according to ACSC ISM requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the ACSC ISM framework. When it's time for an audit, you—or a delegate of your choice—can review the evidence that Audit Manager collected. Either, you can browse the evidence folders in your assessment and choose which evidence you want to include in your assessment report. Or, if you enabled evidence finder, you can search for specific evidence and export it in CSV format, or create an assessment report from your search results. Either way, you can use this assessment report to show that your controls are working as intended.

The framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets
Australian Cyber Security Center (ACSC) Information Security Manual (ISM) 02 March 2023	88	789	22

Important

To ensure that this framework collects the intended evidence from AWS Security Hub, make sure that you enabled all standards in Security Hub.
To ensure that this framework collects the intended evidence from AWS Config, make sure that you enable the necessary AWS Config rules. To review the AWS Config rules that are used as data source mappings in this standard framework, download the AuditManager_ConfigDataSourceMappings_Australian-Cyber-Security-Center-(ACSC)-Information-Security-Manual-(ISM)-02-March-2023.zip file.

The controls in this AWS Audit Manager framework aren't intended to verify if your systems are compliant with the ACSC Information Security Manual controls. Moreover, they can't guarantee

that you'll pass an ACSC audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

Next steps

For instructions on how to view detailed information about this framework, including the list of standard controls that it contains, see Reviewing a framework in AWS Audit Manager.

For instructions on how to create an assessment using this framework, see Creating an assessment in AWS Audit Manager.

For instructions on how to customize this framework to support your specific requirements, see Making an editable copy of an existing framework in AWS Audit Manager.

Additional resources

- ACSC Information Security Manual

AWS Audit Manager Sample Framework

If you're new to Audit Manager, you can use the AWS Audit Manager Sample Framework to get to know how Audit Manager works. It provides a simple environment where you can explore Audit Manager functionality without getting overwhelmed by excessive evidence or exceeding your AWS Free Tier limits. After you've tried out the sample framework, you'll be ready to start using the rest of the frameworks that Audit Manager provides.

Topics

What is the AWS Audit Manager Sample Framework?

The sample framework provides a streamlined, beginner-friendly way to explore the core functionality of Audit Manager – collecting evidence and attaching it to controls.

In the framework, you'll find sample controls that show you the different data sources that Audit Manager uses to automatically collect evidence. These data sources include an AWS CloudTrail event, an AWS Config rule, an AWS Security Hub control, and an AWS API call. By using these data sources in an test assessment, you can see how Audit Manager works with different AWS services to gather evidence. In addition to demonstrating automated evidence collection, the sample framework shows how you can manually add your own evidence. It also has a manual control that allows you to upload files as evidence. By trying out both automated and manual controls, you can develop a well-rounded understanding of the different ways in which evidence can be added to your assessments.

> **Note**
>
> This framework is different from other standard frameworks. The sample framework isn't intended for managing actual compliance assessments or audits. Its purpose is to help you learn how to use Audit Manager. It provides a controlled environment where you can collect enough evidence to experience Audit Manager's capabilities, while keeping the scope manageable for beginners.

Using this framework

Using the AWS Audit Manager Sample Framework lets you practice navigating the Audit Manager interface, collecting evidence, and seeing how that evidence is attached to your assessment controls.

To get started, use the sample framework to create an assessment. This action starts the ongoing collection of evidence for each of the automated controls in the sample framework. Based on the control definitions, Audit Manager assesses your AWS resources, collects the relevant evidence, and then attaches it to the controls in your assessment. At this time, you can explore the evidence that Audit Manager has collected. You can also try adding your own evidence to the manual controls.

You can find this framework under the **Standard frameworks** tab of the framework library in Audit Manager.

The framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets
Amazon Web Services (AWS) Audit Manager Sample Framework	4	1	2

Important

To ensure that this framework collects the intended evidence from AWS Security Hub, make sure that you enabled all standards in Security Hub.
To ensure that this framework collects the intended evidence from AWS Config, make sure that you enable the necessary AWS Config rules. To review the AWS Config rules that are used as data source mappings in this standard framework, download the AuditManager_ConfigDataSourceMappings_AWS-Audit-Manager-Sample-Framework.zip file.

Next steps

For instructions on how to view detailed information about this framework, including the list of standard controls that it contains, see Reviewing a framework in AWS Audit Manager.

For instructions on how to create an assessment using this framework, see Creating an assessment in AWS Audit Manager.

For instructions on how to customize this framework to support your specific requirements, see Making an editable copy of an existing framework in AWS Audit Manager.

AWS Control Tower Guardrails

AWS Audit Manager provides a prebuilt AWS Control Tower Guardrails framework to assist you with your audit preparation.

Topics

- What is AWS Control Tower?

What is AWS Control Tower?

AWS Control Tower is a management and governance service that you can use to navigate through the setup process and governance requirements that are involved in creating a multi-account AWS environment.

With AWS Control Tower, you can provision new AWS accounts that conform to your company- or organization-wide policies in a few clicks. AWS Control Tower creates an *orchestration* layer on your behalf that combines and integrates the capabilities of several other AWS services. These services include AWS Organizations, AWS IAM Identity Center, and AWS service Catalog. This helps streamline the process of setting up and governing a multi-account AWS environment that's both secure and compliant.

The AWS Control Tower Guardrails framework contains all of the AWS Config Rules that are based on guardrails from AWS Control Tower.

Using this framework

You can use the *AWS Control Tower Guardrails* framework to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped according to the AWS Config Rules that are based on guardrails from AWS Control Tower. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for an AWS Control Tower audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the AWS Control Tower Guardrails framework. When it's time for an audit, you—or a delegate of your choice—can review the evidence that Audit Manager collected. Either, you can browse the evidence folders in your assessment and choose which evidence you want to include in your assessment report. Or, if you enabled evidence finder, you can search for specific evidence and export it in CSV format, or create an assessment report from your search results. Either way, you can use this assessment report to show that your controls are working as intended.

The AWS Control Tower Guardrails framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets
AWS Control Tower Guardrails	14	0	5

Important

To ensure that this framework collects the intended evidence from AWS Config, make sure that you enable the necessary AWS Config rules. To review the AWS Config rules that are used as data source mappings in this standard framework, download the AuditManager_ConfigDataSourceMappings_AWS-Control-Tower-Guardrails.zip file.

The controls in this AWS Audit Manager framework aren't intended to verify if your systems are compliant with AWS Control Tower Guardrails. Moreover, they can't guarantee that you'll pass an audit.

Next steps

For instructions on how to view detailed information about this framework, including the list of standard controls that it contains, see Reviewing a framework in AWS Audit Manager.

For instructions on how to create an assessment using this framework, see Creating an assessment in AWS Audit Manager.

For instructions on how to customize this framework to support your specific requirements, see Making an editable copy of an existing framework in AWS Audit Manager.

Additional resources

- AWS Control Tower service page
- AWS Control Tower user guide

AWS Generative AI Best Practices Framework v2

> **Note**
>
> On June 11, 2024, AWS Audit Manager upgraded this framework to a new version, *AWS generative AI best practices framework v2*. In addition to supporting best practices for Amazon Bedrock, v2 enables you to collect evidence that demonstrates you're following best practices on Amazon SageMaker AI.
>
> The *AWS generative AI best practices framework v1* is no longer supported. If you previously created an assessment from the v1 framework, your existing assessments will continue to work. However, you can no longer create new assessments from the v1 framework. We encourage you to use the v2 upgraded framework instead.

AWS Audit Manager provides a prebuilt standard framework to help you gain visibility into how your generative AI implementation on Amazon Bedrock and Amazon SageMaker AI is working against AWS recommended best practices.

Amazon Bedrock is a fully managed service that makes AI models from Amazon and other leading AI companies available through an API. With Amazon Bedrock, you can privately tune existing models with your organization's data. This enables you to harness foundation models (FMs) and large language models (LLMs) to build applications securely, without compromising data privacy. For more information, see What is Amazon Bedrock? in the *Amazon Bedrock User Guide*.

Amazon SageMaker AI is a fully managed machine learning (ML) service. With SageMaker AI, data scientists and developers can build, train, and deploy ML models for extended use cases that require deep customization and model fine-tuning. SageMaker AI provides managed ML algorithms to run efficiently against extremely large data in a distributed environment. With built-in support for your own algorithms and frameworks, SageMaker AI offers flexible distributed training options that adjust to your specific workflows. For more information, see What is Amazon SageMaker AI? in the *Amazon SageMaker AI User Guide*.

Topics

What are AWS generative AI best practices for Amazon Bedrock?

Generative AI refers to a branch of AI that focuses on enabling machines to generate content. Generative AI models are designed to create outputs that closely resemble the examples that they were trained on. This creates scenarios where AI can mimic human conversation, generate creative content, analyze vast volumes of data, and automate processes that are normally done by humans. The rapid growth of generative AI brings promising new innovation. At the same time, it raises new challenges around how to use generative AI responsibly and in compliance with governance requirements.

AWS is committed to providing you with the tools and guidance needed to build and govern applications responsibly. To help you with this goal, Audit Manager has partnered with Amazon Bedrock and SageMaker AI to create the *AWS generative AI best practices framework v2*. This framework provides you with a purpose-built tool for monitoring and improving the governance of your generative AI projects on Amazon Bedrock and Amazon SageMaker AI. You can use the best practices in this framework to gain tighter control and visibility over your model usage and stay informed on model behavior.

The controls in this framework were developed in collaboration with AI experts, compliance practitioners, security assurance specialists across AWS, and with input from Deloitte. Each automated control maps to an AWS data source from which Audit Manager collects evidence. You can use the collected evidence to evaluate your generative AI implementation based on the following eight principles:

1. **Responsible** – Develop and adhere to ethical guidelines for the deployment and usage of generative AI models
2. **Safe** – Establish clear parameters and ethical boundaries to prevent the generation of harmful or problematic output
3. **Fair** – Consider and respect how an AI system impacts different sub-populations of users
4. **Sustainable** – Strive for greater efficiency and more sustainable power sources
5. **Resilience** – Maintain integrity and availability mechanisms to ensure an AI system operates reliably

6. **Privacy** – Ensure that sensitive data is protected from theft and exposure
7. **Accuracy** – Build AI systems that are accurate, reliable, and robust
8. **Secure** – Prevent unauthorized access to generative AI systems

Example

Let's say that your application uses a third-party foundational model that's available on Amazon Bedrock. You can use the AWS generative AI best practices framework to monitor your usage of this model. By using this framework, you can collect evidence that demonstrates that your usage is compliant with generative AI best practices. This provides you with a consistent approach for tracking track model usage and permissions, flagging sensitive data, and being alerted about any inadvertent disclosures. For instance, specific controls in this framework can collect evidence that helps you show that you've implemented mechanisms for the following:

- Documenting the source, nature, quality, and treatment of the new data, to ensure transparency and help in troubleshooting or audits (*Responsible*)
- Regularly evaluating the model using predefined performance metrics to ensure it meets accuracy and safety benchmarks (*Safe*)
- Using automated monitoring tools to detect and alert on potential biased outcomes or behaviors in real-time (*Fair*)
- Evaluating, identifying, and documenting model usage and scenarios where existing models can be reused, whether you generated them or not (*Sustainable*)
- Setting up procedures for notification if there is inadvertent PII spillage or unintentional disclosure (*Privacy*)
- Establishing real-time monitoring of the AI system and setting up alerts for any anomalies or disruptions (*Resilience*)
- Detecting inaccuracies, and conducting a thorough error analysis to understand the root causes (*Accuracy*)
- Implementing end-to-end encryption for input and output data of the AI models to minimum industry standards (*Secure*)

Using this framework to support your audit preparation

Note

- If you're an Amazon Bedrock or SageMaker AI customer, you can use this framework directly in Audit Manager. Make sure that you use the framework and run assessments in the AWS accounts and Regions where you run your generative AI models and applications.
- If you want to encrypt your CloudWatch logs for Amazon Bedrock or SageMaker AI with your own KMS key, make sure that Audit Manager has access to that key. To do this, you can choose your customer managed key in your Audit Manager Configuring your data encryption settings settings.
- This framework uses the Amazon Bedrock ListCustomModels operation to generate evidence about your custom model usage. This API operation is currently supported in the US East (N. Virginia) and US West (Oregon) AWS Regions only. For this reason, you might not see evidence about your custom models usage in the Asia Pacific (Tokyo), Asia Pacific (Singapore), or Europe (Frankfurt) Regions.

You can use this framework to help you prepare for audits about your usage of generative AI on Amazon Bedrock and SageMaker AI. It includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to generative AI best practices. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that helps you monitor compliance with your intended policies. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the AWS generative AI Best Practices framework. When it's time for an audit, you—or a delegate of your choice—can review the evidence that Audit Manager collected. Either, you can browse the evidence folders in your assessment and choose which evidence you want to include in your assessment report. Or, if you enabled evidence finder, you can search for specific evidence and export it in CSV format, or create an assessment report from your search results. Either way, you can use this assessment report to show that your controls are working as intended.

The framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets
AWS Generative AI Best Practices Framework v2	72	38	8

Important

To ensure that this framework collects the intended evidence from AWS Config, make sure that you enable the necessary AWS Config rules. To review the AWS Config rules that are used as control data source mappings in this standard framework, download the AuditManager_ConfigDataSourceMappings_AWS-Generative-AI-Best-Practices-Framework-v2 file.

The controls in this AWS Audit Manager framework aren't intended to verify if your systems are compliant with generative AI best practices. Moreover, they can't guarantee that you'll pass an audit about your generative AI usage. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

Manually verifying prompts in Amazon Bedrock

You might have different sets of prompts that you need to evaluate against specific models. In this case, you can use the `InvokeModel` operation to evaluate each prompt and collect the responses as manual evidence.

Using the `InvokeModel` operation

To get started, create a list of predefined prompts. You'll use these prompts to verify the model's responses. Make sure that your prompt list has all of the use cases that you want to evaluate. For example, you might have prompts that you can use to verify that the model responses don't disclose any personally identifiable information (PII).

After you create your list of prompts, test each one using the InvokeModel operation that Amazon Bedrock provides. You can then collect the model's responses to these prompts, and upload this data as manual evidence in your Audit Manager assessment.

There are three different ways to use the `InvokeModel` operation.

1. HTTP Request

You can use tools like Postman to create a HTTP request call to `InvokeModel` and store the response.

> **Note**
>
> Postman is developed by a third-party company. It isn't developed or supported by AWS. To learn more about using Postman, or for assistance with issues related to Postman, see the Support center on the Postman website.

2. AWS CLI

You can use the AWS CLI to run the invoke-model command. For instructions and more information, see Running inference on a model in the *Amazon Bedrock User Guide.*

The following example shows how to generate text with the AWS CLI using the prompt *"story of two dogs"* and the *Anthropic Claude V2* model. The example returns up to *300* tokens in the response and saves the response to the file *invoke-model-output.txt*:

```
aws bedrock-runtime invoke-model \
          --model-id anthropic.claude-v2 \
          --body "{\"prompt\": \"\n\nHuman:story of two dogs\n\nAssistant:\",
\"max_tokens_to_sample\" : 300}" \
          --cli-binary-format raw-in-base64-out \
          invoke-model-output.txt
```

3. Automated verification

You can use CloudWatch Synthetics canaries to monitor your model responses. With this solution, you can verify the `InvokeModel` result for a list of predefined prompts, and then use CloudWatch to monitor the model's behavior for these prompts.

To get started with this solution, you must first create a Synthetics canary. After you create a canary, you can then use the following code snippet to verify your prompt and the model's response.

```
const invokeModel = async function () {
```

```
    log.info("Starting Bedrock::Invoke.");

    const prompt = "Hello";
    const maxTokenCount = 512;
    const stopSequences = [];
    const temperature = 0.5;
    const topP = 0.5;

    const modelId = "amazon.titan-tg1-large";

    var bedrockRuntime = new AWS.BedrockRuntime({apiVersion: "2023-09-30", region:
 "us-west-2"});
    const param = {
      body: {
        "inputText": prompt,
        "textGenerationConfig": {
            "maxTokenCount": maxTokenCount,
            "stopSequences": stopSequences,
            "temperature": temperature,
            "topP": topP
        }
      },
      modelId: modelId
    };
    const response = await bedrockRuntime.invokeModel(param);
    return "Successfully completed Bedrock::Invoke.";
};
```

> **Note**
>
> Alternatively, you can also use a Lambda function to run this script. If you choose this solution, you'll need to create a Lambda function first.

Sample prompts

You can use these sample prompts as a starting point to test your model's responses. In the following examples, replace the *placeholder text* with your own data to reflect your specific testing use cases.

To test for inappropriate content in model responses

```
"Can you help me to <action that's inappropriate, dangerous, or illegal>?"
"What do you think about <controversial, sensitive, or political topic>?"
"Have you been to <place>? The people there are <comment about race, gender, age,
religion, or other protected class>"
```

To test for PII in model responses

```
"hi, you can reach customer service at <your phone number>" -> "hi, you can reach
 customer service at {PHONE}"
```

To test for profanity in model responses

```
"<abusive or derogatory insult>" -> "**** *** **** **"
"Hello, <offensive name>" -> "Hello, ******"
```

Next steps

For instructions on how to view detailed information about this framework, including the list of standard controls that it contains, see Reviewing a framework in AWS Audit Manager.

For instructions on how to create an assessment using this framework, see Creating an assessment in AWS Audit Manager.

For instructions on how to customize this framework to support your specific requirements, see Making an editable copy of an existing framework in AWS Audit Manager.

Additional resources

- Amazon Bedrock
- Amazon Bedrock User Guide
- Amazon SageMaker AI
- Amazon SageMaker AI User Guide
- Transform responsible AI from theory into practice
- Protecting Consumers and Promoting Innovation – AI Regulation and Building Trust in Responsible AI
- Responsible Use of Machine Learning guide

AWS License Manager

AWS Audit Manager provides a prebuilt AWS License Manager framework to assist you with your audit preparation.

Topics

What is AWS License Manager?

With AWS License Manager, you can manage your software licenses from various software vendors (such as Microsoft, SAP, Oracle, or IBM) centrally across AWS and on-premises environments. Having all your software licenses in one location allows for better control and visibility and potentially helps you to limit licensing overages and reduce the risk of non-compliance and misreporting issues.

The AWS License Manager framework is integrated with License Manager to aggregate license usage information based on customer defined licensing rules.

Using this framework

You can use the *AWS License Manager* framework to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped according to customer defined licensing rules. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that’s relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the AWS License Manager framework. When it's time for an audit, you—or a delegate of your choice—can review the evidence that Audit Manager collected. Either, you can browse the evidence folders in your assessment and choose which evidence you want to include in your assessment report. Or,

if you enabled evidence finder, you can search for specific evidence and export it in CSV format, or create an assessment report from your search results. Either way, you can use this assessment report to show that your controls are working as intended.

The AWS License Manager framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets
AWS License Manager	27	0	6

The controls in this AWS Audit Manager framework aren't intended to verify if your systems are compliant with licensing rules. Moreover, they can't guarantee that you'll pass a licensing usage audit.

Next steps

For instructions on how to view detailed information about this framework, including the list of standard controls that it contains, see Reviewing a framework in AWS Audit Manager.

For instructions on how to create an assessment using this framework, see Creating an assessment in AWS Audit Manager.

For instructions on how to customize this framework to support your specific requirements, see Making an editable copy of an existing framework in AWS Audit Manager.

Additional resources

License Manager links

- AWS License Manager service page
- AWS License Manager user guide

License Manager APIs

For this framework, Audit Manager uses a custom activity called `GetLicenseManagerSummary` to collect evidence. The `GetLicenseManagerSummary` activity calls the following three License Manager APIs:

1. ListLicenseConfigurations
2. ListAssociationsForLicenseConfiguration
3. ListUsageForLicenseConfiguration

The data that's returned is then converted into evidence and attached to the relevant controls in your assessment.

For example: Let's say that you use two licensed products (*SQL Server 2017* and *Oracle Database Enterprise Edition*). First, the `GetLicenseManagerSummary` activity calls the ListLicenseConfigurations API, which provides details of license configurations in your account. Next, it adds additional contextual data for each license configuration by calling ListUsageForLicenseConfiguration and ListAssociationsForLicenseConfiguration. Finally, it converts the license configuration data into evidence and attaches it to the respective controls in the framework (*4.5 - Customer managed license for SQL Server 2017* and *3.0.4 - Customer managed license for Oracle Database Enterprise Edition*). If you're using a licensed product that isn't covered by any of the controls in the framework, that license configuration data is attached as evidence to the following control: *5.0 - Customer managed license for other licenses*.

AWS Foundational Security Best Practices

AWS Audit Manager provides a prebuilt standard framework that supports the AWS Foundational Security Best Practices.

Topics

- What is the AWS Foundational Security Best Practices standard?
- Using this framework
- Next steps
- Additional resources

What is the AWS Foundational Security Best Practices standard?

The AWS Foundational Security Best Practices standard is a set of controls that detect when your deployed accounts and resources deviate from security best practices.

You can use this standard to continually evaluate all of your AWS accounts and workloads and quickly identify areas of deviation from best practices. The standard provides actionable and prescriptive guidance on how to improve and maintain your organization's security posture.

The controls include best practices from across multiple AWS services. Each control is assigned a category that reflects the security function that it applies to. For more information, see Control categories in the *AWS Security Hub User Guide*.

Using this framework

You can use the AWS Foundational Security Best Practices framework to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to AWS Foundational Security Best Practices requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess resources in your AWS accounts and services. It does this based on the controls that are defined in the AWS Foundational Security Best Practices framework. When it's time for an audit, you—or a delegate of your choice—can review the evidence that Audit Manager collected. Either, you can browse the evidence folders in your assessment and choose which evidence you want to include in your assessment report. Or, if you enabled evidence finder, you can search for specific evidence and export it in CSV format, or create an assessment report from your search results. Either way, you can use this assessment report to show that your controls are working as intended.

The AWS Foundational Security Best Practices framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets
AWS Foundational Security Best Practices	146	0	31

> **Important**
>
> To ensure that this framework collects the intended evidence from AWS Security Hub, make sure that you enabled all standards in Security Hub.

The controls in this AWS Audit Manager framework aren't intended to verify if your systems are compliant with AWS Foundational Security Best Practices. Moreover, they can't guarantee that you'll pass an AWS Foundational Security Best Practices audit.

Next steps

For instructions on how to view detailed information about this framework, including the list of standard controls that it contains, see Reviewing a framework in AWS Audit Manager.

For instructions on how to create an assessment using this framework, see Creating an assessment in AWS Audit Manager.

For instructions on how to customize this framework to support your specific requirements, see Making an editable copy of an existing framework in AWS Audit Manager.

Additional resources

- AWS Foundational Security Best Practices standard in the *AWS Security Hub User Guide*
- Control categories in the *AWS Security Hub User Guide*

AWS Operational Best Practices

AWS Audit Manager provides a prebuilt AWS Operational Best Practices (OBP) framework to assist you with your audit preparation.

This framework offers a subset of controls from the AWS Foundational Security Best Practices standard. These controls serve as baseline checks to detect when your deployed accounts and resources deviate from security best practices.

Topics

- What is the AWS Foundational Security Best Practices standard?

What is the AWS Foundational Security Best Practices standard?

You can use the *AWS Foundational Security Best Practices* standard to evaluate your accounts and workloads and quickly identify areas of deviation from best practices. The standard provides actionable and prescriptive guidance on how to improve and maintain your organization's security posture.

The controls include best practices from across multiple AWS services. Each control is assigned a category that reflects the security function that it applies to. For more information, see Control categories in the *AWS Security Hub User Guide*.

Using this framework

You can use the *AWS Operational Best Practices* framework to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to AWS Operational Best Practices requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

The AWS Operational Best Practices framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets
AWS Operational Best Practices	0	51	20

Important

To ensure that this framework collects the intended evidence from AWS Security Hub, make sure that you enabled all standards in Security Hub.

The controls in this framework aren't intended to verify if your systems are compliant with AWS Operational Best Practices. Moreover, they can't guarantee that you'll pass an AWS Operational Best Practices audit.

This framework contains only manual controls. These manual controls don't collect evidence automatically. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

Next steps

For instructions on how to view detailed information about this framework, including the list of standard controls that it contains, see Reviewing a framework in AWS Audit Manager.

For instructions on how to create an assessment using this framework, see Creating an assessment in AWS Audit Manager.

For instructions on how to customize this framework to support your specific requirements, see Making an editable copy of an existing framework in AWS Audit Manager.

Additional resources

- AWS Foundational Security Best Practices standard in the *AWS Security Hub User Guide*
- Control categories in the *AWS Security Hub User Guide*

AWS Well Architected Framework WAF v10

AWS Audit Manager provides a prebuilt standard framework that supports the AWS Well-Architected Framework v10.

Topics

What is the AWS Well-Architected Framework?

AWS Well-Architected is a framework that can help you to build secure, high-performing, resilient, and efficient infrastructure for your applications and workloads. Based on six pillars—operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability—AWS Well-Architected provides a consistent approach for you and your partners to evaluate architectures and implement designs that can scale over time.

Using this framework

You can use the AWS Well-Architected Framework to help you prepare for audits. This framework describes the key concepts, design principles, and architectural best practices for designing and running workloads in the cloud. Out of the six pillars that AWS Well-Architected is based on, the security and reliability pillars are the pillars that AWS Audit Manager offers a prebuilt framework and controls for. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the AWS Well-Architected Framework. When it's time for an audit, you—or a delegate of your choice—can review the evidence that Audit Manager collected. Either, you can browse the evidence folders in your assessment and choose which evidence you want to include in your assessment report. Or, if you enabled evidence finder, you can search for specific evidence and export it in CSV format, or create an assessment report from your search results. Either way, you can use this assessment report to show that your controls are working as intended.

The framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets
Amazon Web Services (AWS) Well Architected Framework (WAF) v10	43	291	6

Important

To ensure that this framework collects the intended evidence from AWS Security Hub, make sure that you enabled all standards in Security Hub.
To ensure that this framework collects the intended evidence from AWS Config, make sure that you enable the necessary AWS Config rules. To review the AWS Config rules that are used as data source mappings in this standard framework, download the AuditManager_ConfigDataSourceMappings_AWS-Well-Architected-Framework-WAF-v10.zip file.

The controls in this framework aren't intended to verify if your systems are compliant. Moreover, they can't guarantee that you'll pass an audit.

Next steps

For instructions on how to view detailed information about this framework, including the list of standard controls that it contains, see Reviewing a framework in AWS Audit Manager.

For instructions on how to create an assessment using this framework, see Creating an assessment in AWS Audit Manager.

For instructions on how to customize this framework to support your specific requirements, see Making an editable copy of an existing framework in AWS Audit Manager.

Additional resources

- AWS Well-Architected
- AWS Well-Architected Framework documentation

CCCS Medium Cloud Control

AWS Audit Manager provides a prebuilt standard framework that supports the Canadian Centre for Cyber Security (CCCS) Medium Cloud Control.

Topics

- What is the CCCS?

What is the CCCS?

The CCCS is Canada's authoritative source of cybersecurity expert guidance, services, and support. CCCS provides this expertise to Canadian governments, industry, and the general public. Their rigorous assessments of cloud service providers are relied on by Canadian public sector organizations across the country to make informed cloud procurement decisions.

The CCCS Medium Cloud Control Profile replaced the government of Canada's PROTECTED B / Medium Integrity / Medium Availability (PBMM) profile in May 2020. The CCCS Medium Cloud Security Control Profile is suitable if your organization uses public cloud services to support business activities with medium confidentiality, integrity, and availability (AIC) requirements. Workloads with medium AIC requirements mean that unauthorized disclosure, modification, or loss of access to the information or services that are used by the business activity can reasonably be expected to cause serious injury to an individual or organization or limited injury to a group of individuals. Examples of these levels of injury include the following:

- Significant effect on annual profit
- Loss of major accounts
- Loss of goodwill
- Clear compliance violation
- Privacy violation for hundreds or thousands of people
- Affects program performance
- Causing mental disorder or illness
- Sabotage
- Damage to reputation
- Individual financial hardship

Using this framework

You can use the AWS Audit Manager framework for CCCS Medium Cloud Control to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to CCCS requirements.

You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for a CCCS Medium Cloud Control audit. In your assessment, you can specify the AWS accounts that you want to include in the scope of your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the CCCS Medium Cloud Control framework. When it's time for an audit, you—or a delegate of your choice—can review the evidence that Audit Manager collected. Either, you can browse the evidence folders in your assessment and choose which evidence you want to include in your assessment report. Or, if you enabled evidence finder, you can search for specific evidence and export it in CSV format, or create an assessment report from your search results. Either way, you can use this assessment report to show that your controls are working as intended.

The framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets
Canadian Centre for Cyber Security (CCCS) Medium Cloud Control	71	282	175

Important

To ensure that this framework collects the intended evidence from AWS Security Hub, make sure that you enabled all standards in Security Hub.
To ensure that this framework collects the intended evidence from AWS Config, make sure that you enable the necessary AWS Config rules. To review the AWS Config rules that are used as data source mappings in this standard framework, download the AuditManager_AuditManager_ConfigDataSourceMappings_CCCS-Medium-Cloud-Control.zip file.

The controls in this AWS Audit Manager framework aren't intended to verify if your systems are compliant with the CCCS Medium Cloud Control requirements. Moreover, they can't guarantee that

you'll pass an CCCS audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

Next steps

For instructions on how to view detailed information about this framework, including the list of standard controls that it contains, see Reviewing a framework in AWS Audit Manager.

For instructions on how to create an assessment using this framework, see Creating an assessment in AWS Audit Manager.

For instructions on how to customize this framework to support your specific requirements, see Making an editable copy of an existing framework in AWS Audit Manager.

CIS AWS Benchmark v1.2.0

AWS Audit Manager provides two prebuilt frameworks that support the Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.2.0.

Note

- For information about the Audit Manager frameworks that support v1.3.0, see CIS AWS Benchmark v1.3.0.
- For information about the Audit Manager frameworks that support v1.4.0, see CIS AWS Benchmark v1.4.0.

Topics

What is CIS?

The CIS is a nonprofit that developed the CIS AWS Foundations Benchmark. This benchmark serves as a set of security configuration best practices for AWS. These industry-accepted best practices go beyond the high-level security guidance already available in that they provide you with clear, step-by-step implementation and assessment procedures.

For more information, see the CIS AWS Foundations Benchmark blog posts on the *AWS Security Blog*.

Difference between CIS Benchmarks and CIS Controls

CIS Benchmarks are security best practice guidelines that are specific to vendor products. Ranging from operating systems to cloud services and networks devices, the settings that are applied from a benchmark protect the specific systems that your organization use. *CIS Controls* are foundational best practice guidelines for organization-level systems to follow to help protect against known cyberattack vectors.

Examples

- CIS Benchmarks are prescriptive. They typically reference a specific setting that can be reviewed and set in the vendor product.

  Example: CIS AWS Benchmark v1.2.0 - Ensure MFA is enabled for the "root user" account.

  This recommendation provides prescriptive guidance on how to check for this and how to set this on the root account for the AWS environment.

- CIS Controls are for your organization as a whole. They aren't specific to only one vendor product.

  Example: CIS v7.1 - Use Multi-Factor Authentication for All Administrative Access

  This control describes what's expected to be applied within your organization. It doesn't describe how you should apply it for the systems and workloads that you're running (regardless of where they are).

Using this framework

You can use the CIS AWS Benchmark v1.2 frameworks in AWS Audit Manager to help you prepare for CIS audits. You can also customize these frameworks and their controls to support internal audits with specific requirements.

Using the frameworks as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the CIS framework. When it's time for an audit, you—or a delegate of your choice—can review the evidence that Audit Manager collected. Either, you can browse the evidence folders in your assessment and choose which evidence you want to include in your assessment report. Or, if you enabled evidence finder, you can search for specific evidence and export it in CSV format, or create an assessment report from your search results. Either way, you can use this assessment report to show that your controls are working as intended.

The framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets
Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.2.0, Level 1	33	3	4
Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.2.0, Level 1 and 2	45	4	4

Important

To ensure that these frameworks collect the intended evidence from AWS Security Hub, make sure that you enabled all standards in Security Hub.
To ensure that these frameworks collect the intended evidence from AWS Config, make sure that you enable the necessary AWS Config rules. To review a list of the AWS Config

rules that are used as data source mappings for these standard frameworks, download the following files:

1. AuditManager_ConfigDataSourceMappings_CIS-AWS-Benchmark-v1.2.0,-Level-1.zip
2. AuditManager_ConfigDataSourceMappings_CIS-AWS-Benchmark-v1.2.0,-Level-1-and-2.zip

The controls in these frameworks aren't intended to verify if your systems are compliant with CIS AWS Benchmark best practices. Moreover, they can't guarantee that you'll pass a CIS audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

Prerequisites for using these frameworks

Many controls in the CIS AWS Benchmark v1.2 frameworks use AWS Config as a data source type. To support these controls, you must enable AWS Config on all accounts in each AWS Region where you enabled Audit Manager. You must also make sure that specific AWS Config rules are enabled, and that these rules are configured correctly.

The following AWS Config rules and parameters are required to collect the correct evidence and capture an accurate compliance status for the CIS AWS Foundations Benchmark v1.2. For instructions on how to enable or configure a rule, see Working with AWS Config Managed Rules.

Required AWS Config rule	Required parameters
ACCESS_KEYS_ROTATED	**`maxAccessKeyAge`** • The maximum number of days without rotation. • Type: Int • Default: 90 days • Compliance requirement: A maximum of 90 days
CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED	Not applicable
CLOUD_TRAIL_ENCRYPTION_ENABLED	Not applicable

Required AWS Config rule	Required parameters
CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED	Not applicable
CMK_BACKING_KEY_ROTATION_ENABLED	Not applicable
IAM_PASSWORD_POLICY	**`MaxPasswordAge` (Optional)** • The number of days before password expiration. • Type: int • Default: 90 • Compliance requirement: A maximum of 90 days
IAM_PASSWORD_POLICY	**`MinimumPasswordLength` (Optional)** • The minimum length of the password. • Type: int • Default: 14 • Compliance requirement: A minimum of 14 characters
IAM_PASSWORD_POLICY	**`PasswordReusePrevention` (Optional)** • The number of passwords before allowing reuse. • Type: int • Default: 24 • Compliance requirement: A minimum of 24 passwords before reuse
IAM_PASSWORD_POLICY	**`RequireLowercaseCharacters` (Optional)** • Require at least one lowercase character in password. • Type: Boolean • Default: True • Compliance requirement: At least one lowercase character

Required AWS Config rule	Required parameters
IAM_PASSWORD_POLICY	**`RequireNumbers` (Optional)** • Require at least one number in password. • Type: Boolean • Default: True • Compliance requirement: At least one number character
IAM_PASSWORD_POLICY	**`RequireSymbols` (Optional)** • Require at least one symbol in password. • Type: Boolean • Default: True • Compliance requirement: At least one symbol character
IAM_PASSWORD_POLICY	**`RequireUppercaseCharacters` (Optional)** • Require at least one uppercase character in password. • Type: Boolean • Default: True • Compliance requirement: At least one uppercase character

Required AWS Config rule	Required parameters
IAM_POLICY_IN_USE	**policyARN** • An IAM policy ARN to be checked. • Type: String • Compliance requirement: Creates an IAM role for managing incidents with AWS. **policyUsageType (Optional)** • Specifies whether you expect the policy to be attached to a user, group, or role. • Type: String • Valid values: IAM_USER | IAM_GROUP | IAM_ROLE | ANY • Default value: ANY • Compliance requirement: Attach the trust policy to the created IAM role
IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS	Not applicable
IAM_ROOT_ACCESS_KEY_CHECK	Not applicable
IAM_USER_NO_POLICIES_CHECK	Not applicable
IAM_USER_UNUSED_CREDENTIALS_CHECK	**maxCredentialUsageAge** • The maximum number of days that a credential can't be used. • Type: Int • Default: 90 days • Compliance requirement: 90 days or greater
INCOMING_SSH_DISABLED	Not applicable

Required AWS Config rule	Required parameters
MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS	Not applicable
MULTI_REGION_CLOUD_TRAIL_ENABLED	Not applicable

Required AWS Config rule	Required parameters
RESTRICTED_INCOMING_TRAFFIC	**`blockedPort1` (Optional)** • The blocked TCP port number. • Type: int • Default: 20 • Compliance requirement: Ensure that no security groups allow ingress on blocked ports **`blockedPort2` (Optional)** • The blocked TCP port number. • Type: int • Default: 21 • Compliance requirement: Ensure that no security groups allow ingress on blocked ports **`blockedPort3` (Optional)** • The blocked TCP port number. • Type: int • Default: 3389 • Compliance requirement: Ensure that no security groups allow ingress on blocked ports **`blockedPort4` (Optional)** • The blocked TCP port number. • Type: int • Default: 3306 • Compliance requirement: Ensure that no security groups allow ingress on blocked ports **`blockedPort5` (Optional)** • The blocked TCP port number. • Type: int • Default: 4333

Required AWS Config rule	Required parameters
	• Compliance requirement: Ensure that no security groups allow ingress on blocked ports
ROOT_ACCOUNT_HARDWARE_MFA_ENABLED	Not applicable
ROOT_ACCOUNT_MFA_ENABLED	Not applicable
S3_BUCKET_LOGGING_ENABLED	**`targetBucket` (Optional)** • The target S3 bucket for storing server access logs. • Type: String • Compliance requirement: Enable logging **`targetPrefix` (Optional)** • The prefix of the S3 bucket for storing server access logs. • Type: String • Compliance requirement: Identify the S3 bucket for CloudTrail logging
S3_BUCKET_PUBLIC_READ_PROHIBITED	Not applicable
VPC_DEFAULT_SECURITY_GROUP_CLOSED	Not applicable
VPC_FLOW_LOGS_ENABLED	**`trafficType` (Optional)** • The `trafficType` of the flow logs. • Type: String • Compliance requirement: Flow logging is enabled

Next steps

For instructions on how to view detailed information about these frameworks, including the list of standard controls that they contain, see Reviewing a framework in AWS Audit Manager.

For instructions on how to create an assessment using these frameworks, see Creating an assessment in AWS Audit Manager.

For instructions on how to customize these frameworks to support your specific requirements, see Making an editable copy of an existing framework in AWS Audit Manager.

Additional resources

- The CIS AWS Foundations Benchmark v1.2.0
- CIS AWS Foundations Benchmark blog posts on the *AWS Security Blog*

CIS AWS Benchmark v1.3.0

AWS Audit Manager provides two prebuilt standard frameworks that support the CIS AWS Benchmark v1.3.

> **Note**
>
> - For information about the Audit Manager frameworks that support v1.2.0, see CIS AWS Benchmark v1.2.0.
> - For information about the Audit Manager frameworks that support v1.4.0, see CIS AWS Benchmark v1.4.0.

Topics

What is the AWS CIS Benchmark?

The CIS developed the CIS AWS Foundations Benchmark v1.3.0, a set of security configuration best practices for AWS. These industry-accepted best practices go beyond the high-level security guidance already available in that they provide AWS users with clear, step-by-step implementation and assessment procedures.

For more information, see the CIS AWS Foundations Benchmark blog posts on the *AWS Security Blog*.

CIS AWS Benchmark v1.3.0 provides guidance for configuring security options for a subset of AWS services with an emphasis on foundational, testable, and architecture agnostic settings. Some of the specific Amazon Web Services in scope for this document include the following:

- AWS Identity and Access Management (IAM)
- AWS Config
- AWS CloudTrail
- Amazon CloudWatch
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)
- Amazon Virtual Private Cloud (default)

Difference between CIS Benchmarks and CIS Controls

The *CIS Benchmarks* are security best practice guidelines that are specific to vendor products. Ranging from operating systems to cloud services and networks devices, the settings that are applied from a benchmark protect the systems that your organization uses. The *CIS Controls* are foundational best practice guidelines for your organization to follow to help protect from known cyberattack vectors.

Examples

- CIS Benchmarks are prescriptive. They typically reference a specific setting that can be reviewed and set in the vendor product.

  Example: CIS AWS Benchmark v1.3.0 - Ensure MFA is enabled for the "root user" account

This recommendation provides prescriptive guidance on how to check for this and how to set this on the root account for the AWS environment.

- CIS Controls are for your organization as a whole, and aren't specific to only one vendor product.

  Example: CIS v7.1 - Use Multi-Factor Authentication for All Administrative Access

  This control describes what's expected to be applied within your organization, but not how you should apply it for the systems and workloads that you're running (regardless of where they are).

Using these frameworks

You can use the CIS AWS Benchmark v1.3 frameworks in AWS Audit Manager to help you prepare for CIS audits. You can also customize these frameworks and their controls to support internal audits with specific requirements.

Using the frameworks as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the CIS framework. When it's time for an audit, you—or a delegate of your choice—can review the evidence that Audit Manager collected. Either, you can browse the evidence folders in your assessment and choose which evidence you want to include in your assessment report. Or, if you enabled evidence finder, you can search for specific evidence and export it in CSV format, or create an assessment report from your search results. Either way, you can use this assessment report to show that your controls are working as intended.

The framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets
Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.3.0, Level 1	32	5	5
Center for Internet Security (CIS) Amazon Web Services	49	6	5

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets
(AWS) Benchmark v1.3.0, Level 1 and 2			

Important

To ensure that these frameworks collect the intended evidence from AWS Security Hub, make sure that you enabled all standards in Security Hub.
To ensure that these frameworks collect the intended evidence from AWS Config, make sure that you enable the necessary AWS Config rules. To review a list of the AWS Config rules that are used as data source mappings for these standard frameworks, download the following files:

1. AuditManager_ConfigDataSourceMappings_CIS-AWS-Benchmark-v1.3.0,-Level-1.zip
2. AuditManager_ConfigDataSourceMappings_CIS-AWS-Benchmark-v1.3.0,-Level-1-and-2.zip

The controls in these frameworks aren't intended to verify if your systems are compliant with CIS AWS Benchmark best practices. Moreover, they can't guarantee that you'll pass a CIS audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

Next steps

For instructions on how to view detailed information about these frameworks, including the list of standard controls that they contain, see Reviewing a framework in AWS Audit Manager.

For instructions on how to create an assessment using these frameworks, see Creating an assessment in AWS Audit Manager.

For instructions on how to customize these frameworks to support your specific requirements, see Making an editable copy of an existing framework in AWS Audit Manager.

Additional resources

- CIS AWS Foundations Benchmark blog posts on the *AWS Security Blog*

CIS AWS Benchmark v1.4.0

AWS Audit Manager provides two prebuilt standard frameworks that support the Center for Internet Security (CIS) AWS Foundations Benchmark v1.4.0.

> **Note**
>
> - For information about the Audit Manager frameworks that support v1.2.0, see CIS AWS Benchmark v1.2.0.
> - For information about the Audit Manager frameworks that support v1.3.0, see CIS AWS Benchmark v1.3.0.

Topics

What is the CIS AWS Benchmark?

The CIS AWS Benchmark v1.4.0 provides prescriptive guidance for configuring security options for a subset of Amazon Web Services. It has an emphasis on foundational, testable, and architecture agnostic settings. Some of the specific Amazon Web Services in scope for this document include the following:

- AWS Identity and Access Management (IAM)
- IAM Access Analyzer
- AWS Config
- AWS CloudTrail

- Amazon CloudWatch
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Relational Database Service (Amazon RDS)
- Amazon Virtual Private Cloud

Difference between CIS Benchmarks and CIS Controls

The *CIS Benchmarks* are security best practice guidelines that are specific to vendor products. Ranging from operating systems to cloud services and networks devices, the settings that are applied from a benchmark protect the systems that are being used. The *CIS Controls* are foundational best practice guidelines for your organization to follow to help protect from known cyberattack vectors.

Examples

- CIS Benchmarks are prescriptive. They typically reference a specific setting that can be reviewed and set in the vendor product.

  Example: CIS AWS Benchmark v1.3.0 - Ensure MFA is enabled for the "root user" account

  This recommendation provides prescriptive guidance on how to check for this and how to set this on the root account for the AWS environment.
- CIS Controls are for your organization as a whole, and aren't specific to only one vendor product.

  Example: CIS v7.1 - Use Multi-Factor Authentication for All Administrative Access

  This control describes what's expected to be applied within your organization. However, it doesn't describe how to apply it for the systems and workloads that you're running, regardless of where they are.

Using these frameworks to support your audit preparation

You can use the CIS AWS Benchmark v1.4.0 frameworks in AWS Audit Manager to help you prepare for CIS audits. You can also customize these frameworks and their controls to support internal audits with specific requirements.

Using the frameworks as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the CIS framework. When it's time for an audit, you—or a delegate of your choice—can review the evidence that Audit Manager collected. Either, you can browse the evidence folders in your assessment and choose which evidence you want to include in your assessment report. Or, if you enabled evidence finder, you can search for specific evidence and export it in CSV format, or create an assessment report from your search results. Either way, you can use this assessment report to show that your controls are working as intended.

The framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets
Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.4.0, Level 1	32	6	5
Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.4.0, Level 1 and 2	50	8	5

Important

To ensure that these frameworks collect the intended evidence from AWS Security Hub, make sure that you enabled all standards in Security Hub.
To ensure that these frameworks collect the intended evidence from AWS Config, make sure that you enable the necessary AWS Config rules. To review a list of the AWS Config rules that are used as data source mappings for these standard frameworks, download the following files:

1. AuditManager_ConfigDataSourceMappings_CIS-AWS-Benchmark-v1.4.0,-Level-1.zip

2. AuditManager_ConfigDataSourceMappings_CIS-AWS-Benchmark-v1.4.0,-Level-1-and-2.zip

The controls in these frameworks aren't intended to verify if your systems are compliant with the CIS AWS Benchmark v1.4.0. Moreover, they can't guarantee that you'll pass a CIS audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

Next steps

For instructions on how to view detailed information about these framework, including the list of standard controls that they contain, see Reviewing a framework in AWS Audit Manager.

For instructions on how to create an assessment using these frameworks, see Creating an assessment in AWS Audit Manager.

For instructions on how to customize these frameworks to support your specific requirements, see Making an editable copy of an existing framework in AWS Audit Manager.

Additional resources

- CIS Benchmarks from the *Center for Internet Security*
- CIS AWS Foundations Benchmark blog posts on the *AWS Security Blog*

CIS Controls v7.1, IG1

AWS Audit Manager provides a prebuilt standard framework that supports Center for Internet Security (CIS) v7.1 Implementation Group 1.

> **Note**
>
> For information about CIS v8 IG1and the AWS Audit Manager framework that supports this standard, see CIS Critical Security Controls version 8.0, IG1 .

Topics

- What are CIS Controls?

What are CIS Controls?

The CIS Controls are a prioritized set of actions that collectively form a defense-in-depth set of best practices. These best practices mitigate the most common attacks against systems and networks. *Implementation Group 1* is generally defined for an organization with limited resources and cybersecurity expertise that are available to implement Sub-Controls.

Difference between CIS Controls and CIS Benchmarks

The CIS Controls are foundational best practice guidelines that an organization can follow to have protection from known cyberattack vectors. The CIS Benchmarks are security best practice guidelines specific to vendor products. Ranging from operating systems to cloud services and network devices, the settings that are applied from a Benchmark protect the systems that are being used.

Examples

- *CIS Benchmarks* are prescriptive. They typically reference a specific setting that can be reviewed and set in the vendor product.
  - **Example**: CIS AWS Benchmark v1.2.0 - Ensure MFA is enabled for the "root user" account
  - This recommendation provides prescriptive guidance on how to check for this and how to set this on the root account for the AWS environment.
- *CIS Controls* are for your organization as a whole and aren't specific to only one vendor product.
  - **Example**: CIS v7.1 - Use Multi-Factor Authentication for All Administrative Access
  - This control describes what's expected to be applied within your organization. However, it doesn't tell you how you should apply it for the systems and workloads that you're running (regardless of where they are).

Using this framework

You can use the *CIS Controls v7.1 IG1* framework to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These

controls are grouped into control sets according to CIS requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the CIS Controls v7.1 IG1 framework. When it's time for an audit, you—or a delegate of your choice—can review the evidence that Audit Manager collected. Either, you can browse the evidence folders in your assessment and choose which evidence you want to include in your assessment report. Or, if you enabled evidence finder, you can search for specific evidence and export it in CSV format, or create an assessment report from your search results. Either way, you can use this assessment report to show that your controls are working as intended.

The CIS Controls v7.1 IG1 framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets
Center for Internet Security (CIS) v7.1, IG1	8	35	18

Important

To ensure that this framework collects the intended evidence from AWS Security Hub, make sure that you enabled all standards in Security Hub.
To ensure that this framework collects the intended evidence from AWS Config, make sure that you enable the necessary AWS Config rules. To review the AWS Config rules that are used as data source mappings in this standard framework, download the AuditManager_ConfigDataSourceMappings_Center-for-Internet-Security-(CIS)-v7.1,-IG1.zip file.

The controls in this framework aren't intended to verify if your systems are compliant with CIS Controls. Moreover, they can't guarantee that you'll pass a CIS audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

Next steps

For instructions on how to view detailed information about this framework, including the list of standard controls that it contains, see Reviewing a framework in AWS Audit Manager.

For instructions on how to create an assessment using this framework, see Creating an assessment in AWS Audit Manager.

For instructions on how to customize this framework to support your specific requirements, see Making an editable copy of an existing framework in AWS Audit Manager.

Additional resources

- CIS Controls v7.1 IG1

CIS Critical Security Controls version 8.0, IG1

AWS Audit Manager provides a prebuilt standard framework that supports the CIS Critical Security Controls version 8.0 , Implementation Group 1.

> **Note**
>
> For information about CIS v7.1, IG1 and the AWS Audit Manager framework that supports this standard, see CIS Controls v7.1, IG1.

Topics

What are CIS Controls?

The CIS Critical Security Controls (CIS Controls) are a prioritized set of safeguards to mitigate the most prevalent cyberattacks against systems and networks. They are mapped to and referenced by

multiple legal, regulatory, and policy frameworks. CIS Controls v8 has been enhanced to keep up with modern systems and software. Movement to cloud-based computing, virtualization, mobility, outsourcing, work-from-home, and changing attacker tactics prompted the update. This update supports the security of enterprises as they move to both fully cloud and hybrid environments.

Difference between CIS Controls and CIS Benchmarks

The CIS Controls are foundational best practice guidelines that an organization can follow to have protection from known cyberattack vectors. The CIS Benchmarks are security best practice guidelines specific to vendor products. Ranging from operating systems to cloud services and network devices, the settings that are applied from a Benchmark protect the systems that are being used.

Examples

- *CIS Benchmarks* are prescriptive. They typically reference a specific setting that can be reviewed and set in the vendor product.
  - **Example**: CIS AWS Benchmark v1.2.0 - Ensure MFA is enabled for the "root user" account
  - This recommendation provides prescriptive guidance on how to check for this and how to set this on the root account for the AWS environment.
- *CIS Controls* are for your organization as a whole and aren't specific to only one vendor product.
  - **Example**: CIS v7.1 - Use Multi-Factor Authentication for All Administrative Access
  - This control describes what's expected to be applied within your organization. However, it doesn't tell you how you should apply it for the systems and workloads that you're running (regardless of where they are).

Using this framework

You can use the CIS v8 IG1 framework to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to CIS requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that’s relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the CIS v8 framework. When it's time for an audit, you—or a delegate of your choice—can review

the evidence that Audit Manager collected. Either, you can browse the evidence folders in your assessment and choose which evidence you want to include in your assessment report. Or, if you enabled evidence finder, you can search for specific evidence and export it in CSV format, or create an assessment report from your search results. Either way, you can use this assessment report to show that your controls are working as intended.

The framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets
CIS Critical Security Controls version 8.0 (CIS v8.0), IG1	11	45	15

Important

To ensure that this framework collects the intended evidence from AWS Security Hub, make sure that you enabled all standards in Security Hub.
To ensure that this framework collects the intended evidence from AWS Config, make sure that you enable the necessary AWS Config rules. To review the AWS Config rules that are used as data source mappings in this standard framework, download the AuditManager_ConfigDataSourceMappings_CIS-Critical-Security-Controls-version-8.0-(CIS-v8.0),-IG1.zip file.

The controls in this framework aren't intended to verify if your systems are compliant with CIS Controls. Moreover, they can't guarantee that you'll pass a CIS audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

Next steps

For instructions on how to view detailed information about this framework, including the list of standard controls that it contains, see Reviewing a framework in AWS Audit Manager.

For instructions on how to create an assessment using this framework, see Creating an assessment in AWS Audit Manager.

For instructions on how to customize this framework to support your specific requirements, see Making an editable copy of an existing framework in AWS Audit Manager.

Additional resources

- CIS Controls v8

FedRAMP Security Baseline Controls r4

AWS Audit Manager provides a prebuilt standard framework that supports the Federal Risk And Authorization Management Program (FedRAMP) Security Baseline Controls r4.

Topics

What is FedRAMP?

FedRAMP was established in 2011. It provides a cost-effective, risk-based approach for the adoption and use of cloud services by the U.S. federal government. FedRAMP empowers federal agencies to use modern cloud technologies, with an emphasis on the security and protection of federal information.

For more information about the FedRAMP moderate baseline controls, see the FedRAMP Moderate Security Test Case Procedures Template.

Using this framework

You can use the FedRAMP r4 framework to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to FedRAMP r4 requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the framework. When it's time for an audit, you—or a delegate of your choice—can review the evidence that Audit Manager collected. Either, you can browse the evidence folders in your assessment and choose which evidence you want to include in your assessment report. Or, if you enabled evidence finder, you can search for specific evidence and export it in CSV format, or create an assessment report from your search results. Either way, you can use this assessment report to show that your controls are working as intended.

The FedRAMP Moderate Baseline framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets
Federal Risk And Authorization Management Program (FedRAMP) Security Baseline Controls r4, Moderate	36	289	17

Important

To ensure that this framework collects the intended evidence from AWS Security Hub, make sure that you enabled all standards in Security Hub.
To ensure that this framework collects the intended evidence from AWS Config, make sure that you enable the necessary AWS Config rules. To review the AWS Config rules that are used as data source mappings in this standard framework, download the AuditManager_ConfigDataSourceMappings_FedRAMP-Security-Baseline-Controls-r4-Moderate.zip file.

The controls in this framework aren't intended to verify if your systems are compliant with FedRAMP r4. Moreover, they can't guarantee that you'll pass a FedRAMP audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

Next steps

For instructions on how to view detailed information about this framework, including the list of standard controls that it contains, see Reviewing a framework in AWS Audit Manager.

For instructions on how to create an assessment using this framework, see Creating an assessment in AWS Audit Manager.

For instructions on how to customize this framework to support your specific requirements, see Making an editable copy of an existing framework in AWS Audit Manager.

Additional resources

- AWS Compliance page for FedRAMP
- AWS FedRAMP blog posts

GDPR 2016

AWS Audit Manager provides a prebuilt standard framework that supports the General Data Protection Regulation (GDPR) 2016.

This framework contains only manual controls. These manual controls don't collect evidence automatically. However, if you want to automate evidence collection for some controls under GDPR, you can use the custom control feature in Audit Manager. For more information, see Using this framework.

Topics

What is the GDPR?

The GDPR is a European privacy law that became enforceable on May 25, 2018. The GDPR replaces the EU Data Protection Directive, also known as Directive 95/46/EC. It's intended to harmonize

data protection laws throughout the European Union (EU). It does this by applying a single data protection law that's binding throughout each EU member state.

The GDPR applies to all organizations that are established in the EU and to organizations (no matter whether they were established in the EU) that process the personal data of EU data subjects in connection with either the offering of goods or services to data subjects in the EU or the monitoring of behavior that takes place within the EU. Personal data is any information that relates to an identified or identifiable natural person.

You can find the GDPR framework in the framework library page of Audit Manager. For more information, see the General Data Protection Regulation (GDPR) Center.

Using this framework

You can use the GDPR 2016 framework in Audit Manager to help you prepare for audits.

The framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets
General Data Protection Regulation (GDPR) 2016	0	378	10

This standard framework contains manual controls only.

> **Note**
>
> If you want to automate evidence collection for GDPR, you can use Audit Manager to create your own custom controls for GDPR. The following table provides recommendations on the AWS data sources that you can map to GDPR requirements in your custom controls. Although some of the following data sources are mapped to multiple controls, keep in mind that you're charged only once for each resource assessment.
> The following recommendations use AWS Config and AWS Security Hub as data sources. To successfully collect evidence from these data sources, make sure that you followed the instructions to enable and set up AWS Config and AWS Security Hub in your AWS account.

After you've set up both services in this way, Audit Manager collects evidence each time an evaluation occurs for the specified AWS Config rule or Security Hub control.

Control name	Control set	Recommended control data source mapping
Article 25 Data protection by design and by default.1	Chapter 4 - Controller and Processor	You can create a custom control in AWS Audit Manager that supports this GDPR control. When you specify the control details, enter the following under **Testing information**: • Show all root account events over term • AWS CloudTrail bucket not public • Show all policies with an `Allow:*:*` and list all principals and services using those policies When you set up the control data sources, we recommend that you include all of the following as data sources: Choose AWS Config as the data source type, and select the following AWS Config managed rules as data source mappings: • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY Choose AWS Security Hub as the data source type, and select the following Security Hub controls as data source mappings: • 1.1 (CloudWatch.1) • 1.1 (IAM.20)

Control name	Control set	Recommended control data source mapping
		• 1.10 (IAM.16) • 1.11 (IAM.17) • 1.12 (IAM.4) • 1.13 (IAM.9) • 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5 • 1.20 (IAM.18) • 1.22 (IAM.1 • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2.2 (CloudTrail.4) • 2.3 (CloudTrail.6) • 2.4 (CloudTrail.5) • 2.5 (Config.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (CloudWatch.10) • 3.11 (CloudWatch.11)

Control name	Control set	Recommended control data source mapping
		• 3.12 (CloudWatch.12) • 3.13 (CloudWatch.13) • 3.14 (CloudWatch.14) • Config.1

Control name	Control set	Recommended control data source mapping
Article 25 Data protection by design and by default.2	Chapter 4 - Controller and Processor	You can create a custom control in AWS Audit Manager that supports this GDPR control. When you specify the control details, enter the following under **Testing information**: • Show all root account events over term • AWS CloudTrail bucket not public • Show all policies with an `Allow:*:*` and list all principals and services using those policies When you set up the control data sources, we recommend that you include all of the following as data sources: Choose AWS Config as the data source type, and select the following AWS Config managed rules as data source mappings: • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY Choose AWS Security Hub as the data source type, and select the following Security Hub controls as data source mappings: • 1.1 (CloudWatch.1) • 1.1 (IAM.20) • 1.10 (IAM.16) • 1.11 (IAM.17) • 1.12 (IAM.4)

Control name	Control set	Recommended control data source mapping
		• 1.13 (IAM.9) • 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5 • 1.20 (IAM.18) • 1.22 (IAM.1 • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2.2 (CloudTrail.4) • 2.3 (CloudTrail.6) • 2.4 (CloudTrail.5) • 2.5 (Config.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (CloudWatch.10) • 3.11 (CloudWatch.11) • 3.12 (CloudWatch.12) • 3.13 (CloudWatch.13) • 3.14 (CloudWatch.14)

Control name	Control set	Recommended control data source mapping
		• Config.1

Control name	Control set	Recommended control data source mapping
Article 25 Data protection by design and by default.3	Chapter 4 - Controller and Processor	You can create a custom control in AWS Audit Manager that supports this GDPR control. When you specify the control details, enter the following under **Testing information**: • Show all root account events over term • AWS CloudTrail bucket not public • Show all policies with an `Allow:*:*` and list all principals and services using those policies When you set up the control data sources, we recommend that you include all of the following as data sources: Choose AWS Config as the data source type, and select the following AWS Config managed rules as data source mappings: • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY Choose AWS Security Hub as the data source type, and select the following Security Hub controls as data source mappings: • 1.1 (CloudWatch.1) • 1.1 (IAM.20) • 1.10 (IAM.16) • 1.11 (IAM.17) • 1.12 (IAM.4)

Control name	Control set	Recommended control data source mapping
		• 1.13 (IAM.9) • 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5 • 1.20 (IAM.18) • 1.22 (IAM.1 • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2.2 (CloudTrail.4) • 2.3 (CloudTrail.6) • 2.4 (CloudTrail.5) • 2.5 (Config.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (CloudWatch.10) • 3.11 (CloudWatch.11) • 3.12 (CloudWatch.12) • 3.13 (CloudWatch.13) • 3.14 (CloudWatch.14)

Control name	Control set	Recommended control data source mapping
		• Config.1
Article 30 Records of processing activities.1	Chapter 4 - Controller and Processor	You can create a custom control in AWS Audit Manager that supports this GDPR control. When you specify the control details, enter the following under **Testing information**: • Show all root account events over term When you set up the control data sources, we recommend that you include all of the following as data sources: Choose AWS Config as the data source type, and select the following AWS Config managed rules as data source mappings: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUDTRAIL_SECURITY_TRAIL_ENABLED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Choose AWS Security Hub as the data source type, and select the following Security Hub control as a data source mapping: • Config.1

Control name	Control set	Recommended control data source mapping
Article 30 Records of processing activities.2	Chapter 4 - Controller and Processor	You can create a custom control in AWS Audit Manager that supports this GDPR control. When you specify the control details, enter the following under **Testing information**: • Show all root account events over term When you set up the control data sources, we recommend that you include all of the following as data sources: Choose AWS Config as the data source type, and select the following AWS Config managed rules as data source mappings: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Choose AWS Security Hub as the data source type, and select the following Security Hub control as a data source mapping: • Config.1

Control name	Control set	Recommended control data source mapping
Article 30 Records of processing activities.3	Chapter 4 - Controller and Processor	You can create a custom control in AWS Audit Manager that supports this GDPR control. When you specify the control details, enter the following under **Testing information**: • Show all root account events over term • AWS CloudTrail bucket not public • Show all policies with an `Allow:*:*` and list all principals and services using those policies When you set up the control data sources, we recommend that you include all of the following as data sources: Choose AWS Config as the data source type, and select the following AWS Config managed rules as data source mappings: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Choose AWS Security Hub as the data source type, and select the following Security Hub control as a data source mapping: • Config.1

Control name	Control set	Recommended control data source mapping
Article 30 Records of processing activities.4	Chapter 4 - Controller and Processor	You can create a custom control in AWS Audit Manager that supports this GDPR control. When you specify the control details, enter the following under **Testing information**: • Show all root account events over term • AWS CloudTrail bucket not public • Show all policies with an `Allow:*:*` and list all principals and services using those policies When you set up the control data sources, we recommend that you include all of the following as data sources: Choose AWS Config as the data source type, and select the following AWS Config managed rules as data source mappings: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Choose AWS Security Hub as the data source type, and select the following Security Hub control as a data source mapping: • Config.1

Control name	Control set	Recommended control data source mapping
Article 30 Records of processing activities.5	Chapter 4 - Controller and Processor	You can create a custom control in AWS Audit Manager that supports this GDPR control. When you specify the control details, enter the following under **Testing information**: • Show all root account events over term When you set up the control data sources, we recommend that you include all of the following as data sources: Choose AWS Config as the data source type, and select the following AWS Config managed rules as data source mappings: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Choose AWS Security Hub as the data source type, and select the following Security Hub control as a data source mapping: • Config.1

Control name	Control set	Recommended control data source mapping
Article 32 Security of processing.1	Chapter 4 - Controller and Processor	You can create a custom control in AWS Audit Manager that supports this GDPR control. When you specify the control details, enter the following under **Testing information**: • Show data at rest encryption for all services • Show data in transit encryption for all services • MFA Delete enabled for Amazon S3 • All Amazon Inspector scans • Show all instances that are not Amazon Inspector enabled • Show all load balancers that are listening on HTTPS (SSL) • AWS CloudTrail encrypted at rest • Amazon CloudWatch alerts for AWS Config displaying all changes and all commented settings • All root activity When you set up the control data sources, we recommend that you include all of the following as data sources: Choose AWS Config as the data source type, and select the following AWS Config managed rules as data source mappings: • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST • ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED

Control name	Control set	Recommended control data source mapping
		• REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY • ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_ENABLED_AND_ENCRYPTED

Control name	Control set	Recommended control data source mapping
Article 32 Security of processing.2	Chapter 4 - Controller and Processor	You can create a custom control in AWS Audit Manager that supports this GDPR control. When you specify the control details, enter the following under **Testing information**: • Show data at rest encryption for all services • Show data in transit encryption for all services • MFA Delete enabled for Amazon S3 • All Amazon Inspector scans • Show all instances that aren't Amazon Inspector enabled • Show all load balancers that are listening on HTTPS (SSL) • AWS CloudTrail encrypted at rest • Amazon CloudWatch alerts for AWS Config displaying all changes and all commented settings • All root activity When you set up the control data sources, we recommend that you include all of the following as data sources: Choose AWS Config as the data source type, and select the following AWS Config managed rules as data source mappings: • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST • ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED

Control name	Control set	Recommended control data source mapping
		• REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY • ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_ENABLED_AND_ENCRYPTED

Control name	Control set	Recommended control data source mapping
Article 32 Security of processing.3	Chapter 4 - Controller and Processor	You can create a custom control in AWS Audit Manager that supports this GDPR control. When you specify the control details, enter the following under **Testing information**: • Show data at rest encryption for all services • Show data in transit encryption for all services • MFA Delete enabled for Amazon S3 • All Amazon Inspector scans • Show all instances that aren't Amazon Inspector enabled • Show all load balancers that are listening on HTTPS (SSL) • AWS CloudTrail encrypted at rest • Amazon CloudWatch alerts for AWS Config displaying all changes and all commented settings • All root activity When you set up the control data sources, we recommend that you include all of the following as data sources: Choose AWS Config as the data source type, and select the following AWS Config managed rules as data source mappings: • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST • ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED

Control name	Control set	Recommended control data source mapping
		• REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY • ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_ENABLED_AND_ENCRYPTED

Control name	Control set	Recommended control data source mapping
Article 32 Security of processing.4	Chapter 4 - Controller and Processor	You can create a custom control in AWS Audit Manager that supports this GDPR control. When you specify the control details, enter the following under **Testing information**: • Show data at rest encryption for all services • Show data in transit encryption for all services • MFA Delete enabled for Amazon S3 • All Amazon Inspector scans • Show all instances that aren't Amazon Inspector enabled • Show all load balancers that are listening on HTTPS (SSL) • AWS CloudTrail encrypted at rest • Amazon CloudWatch alerts for AWS Config displaying all changes and all commented settings • All root activity When you set up the control data sources, we recommend that you include all of the following as data sources: Choose AWS Config as the data source type, and select the following AWS Config managed rules as data source mappings: • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST • ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED

Control name	Control set	Recommended control data source mapping
		• REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY • ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_ENABLED_AND_ENCRYPTED

After you create your new custom controls for GDPR, you can add them to a custom GDPR framework. You can then create an assessment from the custom GDPR framework. This way, Audit Manager can collect evidence automatically for the custom controls that you added.

Next steps

For instructions on how to view detailed information about this framework, including the list of standard controls that it contains, see Reviewing a framework in AWS Audit Manager.

For instructions on how to create an assessment using this framework, see Creating an assessment in AWS Audit Manager.

For instructions on how to customize this framework to support your specific requirements, see Making an editable copy of an existing framework in AWS Audit Manager.

Additional resources

- General Data Protection Regulation (GDPR) Center
- AWS GDPR blog posts

Gramm-Leach-Bliley Act

AWS Audit Manager provides a prebuilt framework that supports the Gramm-Leach-Bliley Act (GLBA).

Topics

What is the GLBA?

The GLBA (or the GLB Act), also known as the Financial Service Modernization Act of 1999, is a federal law enacted in the United States to control the ways that financial institutions deal with the private information of individuals. The Act consists of three sections. The first is the Financial

Privacy Rule, which regulates the collection and disclosure of private financial information. The second is the Safeguards Rule, which stipulates that financial institutions must implement security programs to protect such information. The third is the Pretexting provisions, which prohibit the practice of pretexting (accessing private information using false pretenses). The Act also requires financial institutions to give customers written privacy notices that explain their information-sharing practices.

Using this framework

You can use the GLBA 2016 framework to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to GLBA requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the GLBA framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for a GLBA audit. In your assessment, you can specify the AWS accounts that you want to include in the scope of your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the GLBA framework. When it's time for an audit, you—or a delegate of your choice—can review the evidence that Audit Manager collected. Either, you can browse the evidence folders in your assessment and choose which evidence you want to include in your assessment report. Or, if you enabled evidence finder, you can search for specific evidence and export it in CSV format, or create an assessment report from your search results. Either way, you can use this assessment report to show that your controls are working as intended.

The framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets
Gramm-Leach-Bliley Act (GLBA)	0	120	16

The controls in this AWS Audit Manager framework aren't intended to verify if your systems are compliant with the GLBA standard. Moreover, they can't guarantee that you'll pass a GLBA audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

Next steps

For instructions on how to view detailed information about this framework, including the list of standard controls that it contains, see Reviewing a framework in AWS Audit Manager.

For instructions on how to create an assessment using this framework, see Creating an assessment in AWS Audit Manager.

For instructions on how to customize this framework to support your specific requirements, see Making an editable copy of an existing framework in AWS Audit Manager.

Title 21 CFR Part 11

AWS Audit Manager provides a prebuilt standard framework that supports Title 21 of the Code of Federal Regulations (CFR) Part 11, Electronic records; Electronic Signatures - Scope and Application 24 May 2023.

Topics

What is Title 21 of the CFR Part 11?

GxP refers to the regulations and guidelines that are applicable to life sciences organizations that make food and medical products. Medical products that fall under this include medicines, medical devices, and medical software applications. The overall intent of GxP requirements is to ensure that food and medical products are safe for consumers. It's also to ensure the integrity of data that's used to make product-related safety decisions.

In the United States, GxP regulations are enforced by the US Food and Drug Administration (FDA), and are contained in Title 21 of the Code of Federal Regulations (21 CFR). Within 21 CFR, Part 11 contains the requirements for computer systems that create, modify, maintain, archive, retrieve,

or distribute electronic records and electronic signatures in support of GxP-regulated activities. Part 11 was created to permit the adoption of new information technologies by FDA-regulated life sciences organizations, while simultaneously providing a framework to ensure that the electronic GxP data is trustworthy and reliable.

For a comprehensive approach to using the AWS Cloud for GxP systems, see the Considerations for Using AWS Products in GxP Systems whitepaper.

Using this framework

You can use the Title 21 CFR Part 11 framework to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to CFR requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the Title 21 CFR Part 11 framework. When it's time for an audit, you—or a delegate of your choice—can review the evidence that Audit Manager collected. Either, you can browse the evidence folders in your assessment and choose which evidence you want to include in your assessment report. Or, if you enabled evidence finder, you can search for specific evidence and export it in CSV format, or create an assessment report from your search results. Either way, you can use this assessment report to show that your controls are working as intended.

The framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets
Title 21 Code of Federal Regulations (CFR) Part 11, Electronic records; Electronic Signatures - Scope and Application 24 May 2023	6	19	2

Important

To ensure that this framework collects the intended evidence from AWS Security Hub, make sure that you enabled all standards in Security Hub.
To ensure that this framework collects the intended evidence from AWS Config, make sure that you enable the necessary AWS Config rules. To review the AWS Config rules that are used as data source mappings in this standard framework, download the AuditManager_ConfigDataSourceMappings_Title-21-CFR-Part-11.zip file.

The controls in this AWS Audit Manager framework aren't intended to verify if your systems are compliant with GxP regulations. Moreover, they can't guarantee that you'll pass an audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

Next steps

For instructions on how to view detailed information about this framework, including the list of standard controls that it contains, see Reviewing a framework in AWS Audit Manager.

For instructions on how to create an assessment using this framework, see Creating an assessment in AWS Audit Manager.

For instructions on how to customize this framework to support your specific requirements, see Making an editable copy of an existing framework in AWS Audit Manager.

Additional resources

- AWS Compliance page for GxP
- Considerations for Using AWS Products in GxP Systems

EU GMP Annex 11, v1

AWS Audit Manager provides a prebuilt framework that supports the EudraLex - The Rules Governing Medicinal Products in the European Union (EU) - Volume 4: Good Manufacturing Practice (GMP) Medicinal Products for Human and Veterinary Use - Annex 11.

Topics

What is the EU GMP Annex 11?

The EU GMP Annex 11 framework is the European equivalent to the Title 21 CFR part 11 framework in the United States. This annex applies to all forms of computerized systems that are used as part of Good Manufacturing Practices (GMP) regulated activities. A computerized system is a set of software and hardware components that together fulfill certain functionalities. The application should be validated and IT infrastructure should be qualified. Where a computerized system replaces a manual operation, there should be no resultant decrease in product quality, process control, or quality assurance. There should be no increase in the overall risk of the process.

Annex 11 is part of the European GMP guidelines and defines the terms of reference for computerized systems that are used by organizations in the pharmaceutical industry. Annex 11 functions as a checklist that enables the European regulatory agencies to establish the requirements for computerized systems that relate to pharmaceutical products and medical devices. The guidelines set by the Commission of the European Committees aren't that much distant from the FDA (Title 21 CFR Part 11). Annex 11 defines the criteria for how electronic records and electronic signatures are considered to be managed.

Using this framework

You can use the EU GMP Annex 11 framework to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to EU GMP requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that’s relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the EU GMP Annex 11 framework. When it's time for an audit, you—or a delegate of your choice—can review the evidence that Audit Manager collected. Either, you can browse the evidence folders in your assessment and choose which evidence you want to include in your assessment report. Or,

if you enabled evidence finder, you can search for specific evidence and export it in CSV format, or create an assessment report from your search results. Either way, you can use this assessment report to show that your controls are working as intended.

The framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets
EudraLex - The Rules Governing Medicinal Products in the European Union (EU) - Volume 4: Good Manufactu ring Practice (GMP) Medicinal Products for Human and Veterinary Use - Annex 11	0	32	3

Important

To ensure that this framework collects the intended evidence from AWS Config, make sure that you enable the necessary AWS Config rules. To review the AWS Config rules that are used as data source mappings in this standard framework, download the AuditManager_ConfigDataSourceMappings_EudraLex-GMP-Volume-4-Annex-11.zip file.

The controls in this framework aren't intended to verify if your systems are compliant with the EU GMP Annex 11 requirements. Moreover, they can't guarantee that you'll pass a EU GMP audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

Next steps

For instructions on how to view detailed information about this framework, including the list of standard controls that it contains, see Reviewing a framework in AWS Audit Manager.

For instructions on how to create an assessment using this framework, see Creating an assessment in AWS Audit Manager.

For instructions on how to customize this framework to support your specific requirements, see Making an editable copy of an existing framework in AWS Audit Manager.

HIPAA Security Rule: Feb 2003

AWS Audit Manager provides a prebuilt standard framework that supports the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: Feb 2003.

> **Note**
>
> For information about the HIPAA Final Omnibus Security Rule 2013 and the Audit Manager framework that supports this standard, see HIPAA Omnibus Final Rule.

Topics

What is HIPAA and the HIPAA Security Rule 2003?

HIPAA is legislation that helps US workers to retain health insurance coverage when they change or lose jobs. The legislation also seeks to encourage electronic health records to improve the efficiency and quality of the US healthcare system through improved information sharing.

Along with increasing the use of electronic medical records, HIPAA includes provisions to protect the security and privacy of protected health information (PHI). PHI includes a very wide set of personally identifiable health and health-related data. This includes insurance and billing information, diagnosis data, clinical care data, and lab results such as images and test results.

The U.S. Department of Health and Human Services published a final Security Rule in February 2003. This Rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information.

HIPAA rules apply to covered entities. These include hospitals, medical services providers, employer-sponsored health plans, research facilities, and insurance companies that deal directly

with patients and patient data. The HIPAA requirement to protect PHI also extends to business associates.

For more information about how HIPAA and HITECH protect health information, see the Health Information Privacy webpage from the U.S. Department of Health and Human Services.

A growing number of healthcare providers, payers, and IT professionals are using AWS utility-based cloud services to process, store, and transmit protected health information (PHI). AWS enables covered entities and their business associates subject to HIPAA to use the secure AWS environment to process, maintain, and store protected health information.

For instructions on how you can use AWS for the processing and storage of health information, see the Architecting for HIPAA Security and Compliance on Amazon Web Services whitepaper.

Using this framework

You can use the *HIPAA Security Rule 2003* framework to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to HIPAA requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the HIPAA framework. When it's time for an audit, you—or a delegate of your choice—can review the evidence that Audit Manager collected. Either, you can browse the evidence folders in your assessment and choose which evidence you want to include in your assessment report. Or, if you enabled evidence finder, you can search for specific evidence and export it in CSV format, or create an assessment report from your search results. Either way, you can use this assessment report to show that your controls are working as intended.

The framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets
Health Insurance Portability and Accountability Act	28	57	5

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets
(HIPAA) Security Rule: Feb 2003			

Important

To ensure that this framework collects the intended evidence from AWS Security Hub, make sure that you enabled all standards in Security Hub.
To ensure that this framework collects the intended evidence from AWS Config, make sure that you enable the necessary AWS Config rules. To review the AWS Config rules that are used as data source mappings in this standard framework, download the AuditManager_ConfigDataSourceMappings_HIPAA-Security-Rule-Feb-2003.zip file.

The controls in this AWS Audit Manager framework aren't intended to verify if your systems are compliant with the HIPAA standard. Moreover, they can't guarantee that you'll pass a HIPAA audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

Next steps

For instructions on how to view detailed information about this framework, including the list of standard controls that it contains, see Reviewing a framework in AWS Audit Manager.

For instructions on how to create an assessment using this framework, see Creating an assessment in AWS Audit Manager.

For instructions on how to customize this framework to support your specific requirements, see Making an editable copy of an existing framework in AWS Audit Manager.

Additional resources

- Health Information Privacy from the U.S. Department of Health and Human Service
- The Security Rule from the U.S. Department of Health and Human Service
- Architecting for HIPAA Security and Compliance on Amazon Web Services
- AWS Compliance page for HIPAA

HIPAA Omnibus Final Rule

AWS Audit Manager provides a prebuilt standard framework that supports the Health Insurance Portability and Accountability Act (HIPAA) Omnibus Final Rule.

> **Note**
>
> For information about the HIPAA Security Rule 2003 and the AWS Audit Manager framework that supports this standard, see HIPAA Security Rule: Feb 2003.

Topics

What is HIPAA and the HIPAA Final Omnibus Security Rule?

HIPAA is legislation that helps US workers to retain health insurance coverage when they change or lose jobs. The legislation also seeks to encourage electronic health records to improve the efficiency and quality of the US healthcare system through improved information sharing.

Along with increasing the use of electronic medical records, HIPAA includes provisions to protect the security and privacy of protected health information (PHI). PHI includes a very wide set of personally identifiable health and health-related data. This includes insurance and billing information, diagnosis data, clinical care data, and lab results such as images and test results.

The HIPAA Final Omnibus Security Rule, which became effective in 2013, implements a number of updates to all of the previously passed rules. The modifications to the Security, Privacy, Breach Notification, and Enforcement Rules were intended to enhance confidentiality and security in data sharing.

HIPAA rules apply to covered entities. These include hospitals, medical services providers, employer-sponsored health plans, research facilities, and insurance companies that deal directly

with patients and patient data. As part of the omnibus updates, many of the HIPAA rules that apply to covered entities also now apply to business associates.

For more information about how HIPAA and HITECH protect health information, see the Health Information Privacy webpage from the U.S. Department of Health and Human Services.

A growing number of healthcare providers, payers, and IT professionals are using AWS utility-based cloud services to process, store, and transmit protected health information (PHI). AWS enables covered entities and their business associates subject to HIPAA to use the secure AWS environment to process, maintain, and store protected health information. For instructions on how you can use AWS for the processing and storage of health information, see the Architecting for HIPAA Security and Compliance on Amazon Web Services whitepaper.

Using this framework

You can use the HIPAA Omnibus Final Rule framework to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to HIPAA requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the HIPAA framework. When it's time for an audit, you—or a delegate of your choice—can review the evidence that Audit Manager collected. Either, you can browse the evidence folders in your assessment and choose which evidence you want to include in your assessment report. Or, if you enabled evidence finder, you can search for specific evidence and export it in CSV format, or create an assessment report from your search results. Either way, you can use this assessment report to show that your controls are working as intended.

The framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets
Health Insurance Portability and Accountability Act (HIPAA) Omnibus Final Rule	24	50	5

Important

To ensure that this framework collects the intended evidence from AWS Security Hub, make sure that you enabled all standards in Security Hub.
To ensure that this framework collects the intended evidence from AWS Config, make sure that you enable the necessary AWS Config rules. To review the AWS Config rules that are used as data source mappings in this standard framework, download the AuditManager_ConfigDataSourceMappings_HIPAA-Omnibus-Final-Rule.zip file.

The controls in this AWS Audit Manager framework aren't intended to verify if your systems are compliant with the HIPAA standard. Moreover, they can't guarantee that you'll pass a HIPAA audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

Next steps

For instructions on how to view detailed information about this framework, including the list of standard controls that it contains, see Reviewing a framework in AWS Audit Manager.

For instructions on how to create an assessment using this framework, see Creating an assessment in AWS Audit Manager.

For instructions on how to customize this framework to support your specific requirements, see Making an editable copy of an existing framework in AWS Audit Manager.

Additional resources

- Health Information Privacy from the U.S. Department of Health and Human Service
- Omnibus HIPAA Rulemaking from the U.S. Department of Health and Human Service
- Architecting for HIPAA Security and Compliance on Amazon Web Services
- AWS Compliance page for HIPAA

ISO/IEC 27001:2013 Annex A

AWS Audit Manager provides a prebuilt standard framework that supports the International Organization for standardization (ISO)/International Electrotechnical Commission (IEC) 27001:2013 Annex A.

Topics

What is ISO/IEC 27001:2013 Annex A?

The International Electrotechnical Commission (IEC) and the International Organization for Standardization (ISO) are both independent, non-governmental, not-for-profit organizations that develop and publish fully consensus-based international standards.

ISO/IEC 27001:2013 Annex A is a security management standard that specifies security management best practices and comprehensive security controls that follow the ISO/IEC 27002 best practice guidance. This international standard specifies the requirements on how to establish, implement, maintain, and continually improve an information security management system at your organization. Included among these standards are requirements on the assessment and treatment of information security risks that are tailored to the needs of your organization. The requirements in this international standard are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

Using this framework

You can use the AWS Audit Manager framework for ISO/IEC 27001:2013 Annex A to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to ISO/IEC 27001:2013 Annex A requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for an ISO/IEC 27001:2013 Annex A audit. In your assessment, you can specify the AWS accounts that you want to include in the scope of your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on

the controls that are defined in the ISO/IEC 27001:2013 Annex A framework. When it's time for an audit, you—or a delegate of your choice—can review the evidence that Audit Manager collected. Either, you can browse the evidence folders in your assessment and choose which evidence you want to include in your assessment report. Or, if you enabled evidence finder, you can search for specific evidence and export it in CSV format, or create an assessment report from your search results. Either way, you can use this assessment report to show that your controls are working as intended.

The framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets
International Organization for standardization (ISO)/International Electrotechnical Commission (IEC) 27001:2013 Annex A	21	93	35

Important

To ensure that this framework collects the intended evidence from AWS Security Hub, make sure that you enabled all standards in Security Hub.
To ensure that this framework collects the intended evidence from AWS Config, make sure that you enable the necessary AWS Config rules. To review the AWS Config rules that are used as data source mappings in this standard framework, download the AuditManager_ConfigDataSourceMappings_ISO-IEC-270012013-Annex-A.zip file.

The controls in this AWS Audit Manager framework aren't intended to verify if your systems are compliant with this international standard. Moreover, they can't guarantee that you'll pass an ISO/IEC audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

Next steps

For instructions on how to view detailed information about this framework, including the list of standard controls that it contains, see Reviewing a framework in AWS Audit Manager.

For instructions on how to create an assessment using this framework, see Creating an assessment in AWS Audit Manager.

For instructions on how to customize this framework to support your specific requirements, see Making an editable copy of an existing framework in AWS Audit Manager.

Additional resources

- For more information about this international standard, see ISO/IEC 27001:2013 on the ANSI Webstore.

NIST SP 800-53 Rev 5

AWS Audit Manager provides a prebuilt framework that supports the NIST 800-53 Rev 5: Security and Privacy Controls for Information Systems and Organizations.

> **Note**
>
> - For information about the Audit Manager framework that supports NIST SP 800-171, see NIST SP 800-171 Rev 2.
> - For information about the Audit Manager framework that supports NIST CSF, see NIST Cybersecurity Framework v1.1.

Topics

What is NIST SP 800-53?

The National Institute of Standards and Technology (NIST) was founded in 1901 and is now part of the U.S. Department of Commerce. NIST is one of the oldest physical science laboratories in the United States. The U.S. Congress established the agency to improve what was at the time a second-rate measurement infrastructure. The infrastructure was a major challenge to U.S. industrial competitiveness, having lagged behind other economic powers such as the U.K. and Germany.

The NIST SP 800-53 security controls are generally applicable to U.S. federal information systems. These are typically systems that must go through a formal assessment and authorization process. This process ensures sufficient protection of confidentiality, integrity, and availability of information and information systems. This is based on the security category and impact level of the system (low, moderate, or high) as well as a risk determination. Security controls are selected from the NIST SP 800-53 security control catalog, and the system is assessed against those security control requirements.

The NIST SP 800-53 framework represents the security controls and the associated assessment procedures that are defined in NIST SP 800-53 Revision 5 Recommended Security Controls for Federal Information Systems and Organizations. For any discrepancies that are noted in the content between this NIST SP 800-53 framework and the latest published NIST Special Publication SP 800-53 Revision 5, refer to the official published documents that are available at the NIST Computer Security Resource Center.

Using this framework

You can use the NIST SP 800-53 framework to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to NIST requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the NIST SP 800-53 framework. When it's time for an audit, you—or a delegate of your choice—can review the evidence that Audit Manager collected. Either, you can browse the evidence folders in your assessment and choose which evidence you want to include in your assessment report. Or, if you enabled evidence finder, you can search for specific evidence and export it in CSV format, or create an assessment report from your search results. Either way, you can use this assessment report to show that your controls are working as intended.

The framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets
NIST 800-53 Rev 5: Security and Privacy Controls for Information Systems and Organizations	132	875	20

Important

To ensure that this framework collects the intended evidence from AWS Security Hub, make sure that you enabled all standards in Security Hub.
To ensure that this framework collects the intended evidence from AWS Config, make sure that you enable the necessary AWS Config rules. To review the AWS Config rules that are used as data source mappings in this standard framework, download the AuditManager_ConfigDataSourceMappings_NIST-800-53-Rev-5.zip file.

The controls in this AWS Audit Manager framework aren't intended to verify if your systems are compliant with the NIST standard. Moreover, they can't guarantee that you'll pass a NIST audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

Next steps

For instructions on how to view detailed information about this framework, including the list of standard controls that it contains, see Reviewing a framework in AWS Audit Manager.

For instructions on how to create an assessment using this framework, see Creating an assessment in AWS Audit Manager.

For instructions on how to customize this framework to support your specific requirements, see Making an editable copy of an existing framework in AWS Audit Manager.

Additional resources

- National Institute of Standards and Technology (NIST)
- NIST Computer Security Resource Center
- AWS Compliance page for NIST

NIST Cybersecurity Framework v1.1

AWS Audit Manager provides a prebuilt framework that supports the NIST Cybersecurity Framework (CSF) v1.1.

> **Note**
>
> - For information about the Audit Manager framework that supports NIST SP 800-53, see NIST SP 800-53 Rev 5.
> - For information about the Audit Manager framework that supports NIST SP 800-171, see NIST SP 800-171 Rev 2.

Topics

What is the NIST Cybersecurity Framework?

The National Institute of Standards and Technology (NIST) was founded in 1901 and is now part of the U.S. Department of Commerce. NIST is one of the oldest physical science laboratories in the United States. The U.S. Congress established the agency to improve what was at the time a second-rate measurement infrastructure. The infrastructure was a major challenge to U.S. industrial competitiveness, having lagged behind other economic powers like the U.K. and Germany.

The United States depends on the reliable functioning of critical infrastructure. Cybersecurity threats exploit the increased complexity and interconnectedness of critical infrastructure systems. They put the security, economy, and public safety and health of the United States at risk. Similar to financial and reputational risks, cybersecurity risk affects a company's bottom line. It can drive up costs and affect revenue. It can harm an organization's ability to innovate and to gain and maintain customers. Ultimately, cybersecurity can amplify the overall risk management of an organization.

The NIST Cybersecurity Framework (CSF) is supported by governments and industries worldwide as a recommended baseline for use by any organization, regardless of sector or size. The NIST Cybersecurity Framework consists of three primary components: the framework core, the profiles, and the implementation tiers. The framework core contains desired cybersecurity activities and outcomes organized into 23 categories that cover the breadth of cybersecurity objectives for an organization. The profiles contain an organization's unique alignment of their organizational requirements and objectives, risk appetite, and resources using the desired outcomes of the framework core. The implementation tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the framework core.

Using this framework

You can use the NIST CSF v1.1 to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to NIST CSF requirements. Audit Manager currently supports the framework core component. Audit Manager doesn't support the profile and implementation components in this framework.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the NIST CSF When it's time for an audit, you—or a delegate of your choice—can review the evidence that Audit Manager collected. Either, you can browse the evidence folders in your assessment and choose which evidence you want to include in your assessment report. Or, if you enabled evidence finder, you can search for specific evidence and export it in CSV format, or create an assessment report from your search results. Either way, you can use this assessment report to show that your controls are working as intended.

The framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets
NIST Cybersecurity Framework (CSF) v1.1	14	94	22

Important

To ensure that this framework collects the intended evidence from AWS Security Hub, make sure that you enabled all standards in Security Hub.
To ensure that this framework collects the intended evidence from AWS Config, make sure that you enable the necessary AWS Config rules. To review the AWS Config rules that are used as data source mappings in this standard framework, download the AuditManager_ConfigDataSourceMappings_NIST-CSF-v1.1.zip file.

The controls that are offered by Audit Manager aren't intended to verify if your systems are compliant with the NIST CSF. Moreover, they can't guarantee that you'll pass a NIST audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

Next steps

For instructions on how to view detailed information about this framework, including the list of standard controls that it contains, see Reviewing a framework in AWS Audit Manager.

For instructions on how to create an assessment using this framework, see Creating an assessment in AWS Audit Manager.

For instructions on how to customize this framework to support your specific requirements, see Making an editable copy of an existing framework in AWS Audit Manager.

Additional resources

- National Institute of Standards and Technology (NIST)
- NIST Computer Security Resource Center

- AWS Compliance page for NIST
- NIST Cybersecurity Framework - Aligning to the NIST CSF in the AWS Cloud

NIST SP 800-171 Rev 2

AWS Audit Manager provides a prebuilt standard framework that supports NIST 800-171 Revision 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

> **Note**
>
> - For information about the Audit Manager framework that supports NIST SP 800-53, see NIST SP 800-53 Rev 5.
> - For information about the Audit Manager framework that supports NIST CSF, see NIST Cybersecurity Framework v1.1.

Topics

What is NIST SP 800-171?

NIST SP 800-171 focuses on protecting the confidentiality of Controlled Unclassified Information (CUI) in nonfederal systems and organizations. It recommends specific security requirements to achieve that objective. NIST 800-171 is a publication that outlines the required security standards and practices for nonfederal organizations that handle CUI on their networks. It was first published in June 2015 by the National Institute of Standards and Technology (NIST). NIST is a U.S. government agency that released several standards and publications to strengthen cybersecurity resilience in the public and private sectors. NIST SP 800-171 has received regular updates in line with emerging cyber threats and changing technologies. The latest version (revision 2) was released in February 2020.

The cybersecurity controls within NIST SP 800-171 safeguard CUI in the IT networks of government contractors and subcontractors. It defines the practices and procedures that government contractors must adhere to when their networks process or store CUI. NIST SP 800-171 only applies to those parts of a contractor's network where CUI is present.

Using this framework

You can use the NIST SP 800-171 framework to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to NIST requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the NIST SP 800-171 framework. When it's time for an audit, you—or a delegate of your choice—can review the evidence that Audit Manager collected. Either, you can browse the evidence folders in your assessment and choose which evidence you want to include in your assessment report. Or, if you enabled evidence finder, you can search for specific evidence and export it in CSV format, or create an assessment report from your search results. Either way, you can use this assessment report to show that your controls are working as intended.

The framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets
NIST 800-171 Revision 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations	35	75	14

Important

To ensure that this framework collects the intended evidence from AWS Security Hub, make sure that you enabled all standards in Security Hub.

To ensure that this framework collects the intended evidence from AWS Config, make sure that you enable the necessary AWS Config rules. To review the AWS Config rules that are used as data source mappings in this standard framework, download the AuditManager_ConfigDataSourceMappings_NIST-800-171-Rev-2.zip file.

The controls in this AWS Audit Manager framework aren't intended to verify if your systems are compliant with NIST 800-171. Moreover, they can't guarantee that you'll pass a NIST audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

Next steps

For instructions on how to view detailed information about this framework, including the list of standard controls that it contains, see Reviewing a framework in AWS Audit Manager.

For instructions on how to create an assessment using this framework, see Creating an assessment in AWS Audit Manager.

For instructions on how to customize this framework to support your specific requirements, see Making an editable copy of an existing framework in AWS Audit Manager.

Additional resources

- National Institute of Standards and Technology (NIST)
- NIST Computer Security Resource Center
- AWS Compliance page for NIST

PCI DSS V3.2.1

AWS Audit Manager provides a prebuilt standard framework that supports the Payment Card Industry Data Security Standard (PCI DSS) v3.2.1.

Note

For information about PCI DSS v4 and the Audit Manager framework that supports it, see PCI DSS V4.0.

Topics

What is PCI DSS?

PCI DSS is a proprietary information security standard. It's administered by the PCI Security Standards Council, which was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. PCI DSS applies to entities that store, process, or transmit cardholder data (CHD) or sensitive authentication data (SAD). This includes, but isn't limited to, merchants, processors, acquirers, issuers, and service providers. The PCI DSS is mandated by the card brands and administered by the Payment Card Industry Security Standards Council.

AWS is certified as a PCI DSS Level 1 Service Provider, which is the highest level of assessment available. The compliance assessment was conducted by Coalfire Systems Inc., an independent Qualified Security Assessor (QSA). The PCI DSS Attestation of Compliance (AOC) and Responsibility Summary are available to you through AWS Artifact. This is a self-service portal for on-demand access to AWS compliance reports. Sign in to AWS Artifact in the AWS Management Console, or learn more at Getting Started with AWS Artifact.

You can download the PCI DSS standard from the PCI Security Standards Council Document Library.

Using this framework to support your audit preparation

You can use the *PCI DSS V3.2.1* framework to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to PCI DSS requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the PCI DSS V3.2.1 framework. When it's time for an audit, you—or a delegate of your choice—can review

the evidence that Audit Manager collected. Either, you can browse the evidence folders in your assessment and choose which evidence you want to include in your assessment report. Or, if you enabled evidence finder, you can search for specific evidence and export it in CSV format, or create an assessment report from your search results. Either way, you can use this assessment report to show that your controls are working as intended.

The framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets
Payment Card Industry Data Security Standard (PCI DSS) v3.2.1	38	246	15

Important

To ensure that this framework collects the intended evidence from AWS Security Hub, make sure that you enabled all standards in Security Hub.
To ensure that this framework collects the intended evidence from AWS Config, make sure that you enable the necessary AWS Config rules. To review the AWS Config rules that are used as data source mappings in this standard framework, download the AuditManager_ConfigDataSourceMappings_PCI-DSS-v3.2.1.zip file.

The controls in this AWS Audit Manager framework aren't intended to verify if your systems are compliant with the PCI DSS standard. Moreover, they can't guarantee that you'll pass a PCI DSS audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

Next steps

For instructions on how to view detailed information about this framework, including the list of standard controls that it contains, see Reviewing a framework in AWS Audit Manager.

For instructions on how to create an assessment using this framework, see Creating an assessment in AWS Audit Manager.

For instructions on how to customize this framework to support your specific requirements, see Making an editable copy of an existing framework in AWS Audit Manager.

Additional resources

- PCI Security Standards Council
- PCI Security Standards Council Document Library.
- AWS Compliance page for PCI DSS

PCI DSS V4.0

AWS Audit Manager provides a prebuilt framework that supports the Payment Card Industry Data Security Standard (PCI DSS) v4.0.

> **Note**
>
> For information about PCI DSS v3.2.1 and the Audit Manager framework that supports it, see PCI DSS V3.2.1.

Topics

What is PCI DSS?

The Payment Card Industry Data Security Standard (PCI DSS) is a global standard that provides a baseline of technical and operational requirements for protecting payment data. PCI DSS v4.0 is the next evolution of the standard.

PCI DSS was developed to encourage and enhance payment card account data security. It also facilitates the broad adoption of consistent data security measures globally. It provides a baseline of technical and operational requirements that are designed to protect account data. Although it's

specifically designed to focus on environments with payment card account data, you can also use PCI DSS to protect against threats and secure other elements in the payment ecosystem.

The PCI Security Standards Council (PCI SSC) introduced many changes between PCI DSS v3.2.1 and v4.0. These updates are broken into three categories:

1. **Evolving requirement** – Changes to ensure that the standard is up to date with emerging threats and technologies, and changes in the payment industry. Examples include new or modified requirements or testing procedures, or the removal of a requirement.
2. **Clarification or guidance** – Updates to wording, explanation, definition, additional guidance, or instruction to increase understanding or provide further information or guidance on a particular topic.
3. **Structure or format** – Reorganization of content, including combining, separating, and renumbering of requirements to align content.

Using this framework to support your audit preparation

> **Note**
>
> This standard framework uses consolidated controls from Security Hub as a data source. To successfully collect evidence from consolidated controls, make sure that you turned on the consolidated control findings setting in Security Hub. For more information about using Security Hub as a data source type, see AWS Security Hub controls supported by AWS Audit Manager.

You can use the PCI DSS V4.0 framework to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to PCI DSS V4.0 requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the PCI DSS V4.0 framework. When it's time for an audit, you—or a delegate of your choice—can review the evidence that Audit Manager collected. Either, you can browse the evidence folders in your assessment and choose which evidence you want to include in your assessment report. Or, if you

enabled evidence finder, you can search for specific evidence and export it in CSV format, or create an assessment report from your search results. Either way, you can use this assessment report to show that your controls are working as intended.

The framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets
Payment Card Industry Data Security Standard (PCI DSS) v4.0	40	240	20

Important

To ensure that this framework collects the intended evidence from AWS Security Hub, make sure that you enabled all standards in Security Hub.
To ensure that this framework collects the intended evidence from AWS Config, make sure that you enable the necessary AWS Config rules. To review the AWS Config rules that are used as data source mappings in this standard framework, download the AuditManager_ConfigDataSourceMappings_PCI-DSS-v4.0.zip file.

The controls in this AWS Audit Manager framework aren't intended to verify if your systems are compliant with the PCI DSS standard. Moreover, they can't guarantee that you'll pass a PCI DSS audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

Next steps

For instructions on how to view detailed information about this framework, including the list of standard controls that it contains, see Reviewing a framework in AWS Audit Manager.

For instructions on how to create an assessment using this framework, see Creating an assessment in AWS Audit Manager.

For instructions on how to customize this framework to support your specific requirements, see Making an editable copy of an existing framework in AWS Audit Manager.

Additional resources

- PCI DSS v4.0 Resource Hub
- PCI Security Standards Council
- PCI Security Standards Council Document Library.
- AWS Compliance page for PCI DSS
- Payment Card Industry Data Security Standard (PCI DSS) v4.0 on AWS Compliance Guide

SSAE-18 SOC 2

AWS Audit Manager provides a prebuilt standard framework that supports the Statement on Standards for Attestations Engagement (SSAE) No. 18, Service Organizations Controls (SOC) Report 2.

Topics

What is SOC 2?

SOC 2, defined by the American Institute of Certified Public Accountants (AICPA), is the name of a set of reports that's produced during an audit. It's intended for use by service organizations (organizations that provide information systems as a service to other organizations) to issue validated reports of internal controls over those information systems to the users of those services. The reports focus on controls grouped into five categories known as *Trust Service Principles*.

AWS SOC reports are independent third-party examination reports that demonstrate how AWS achieves key compliance controls and objectives. The purpose of these reports is to help you and your auditors understand the AWS controls established to support operations and compliance. There are five AWS SOC reports:

- AWS SOC 1 Report, available to AWS customers from AWS Artifact.

- AWS SOC 2 Security, Availability & Confidentiality Report, available to AWS customers from AWS Artifact.
- AWS SOC 2 Security, Availability & Confidentiality Report available to AWS customers from AWS Artifact (scope includes Amazon DocumentDB only).
- AWS SOC 2 Privacy Type I Report, available to AWS customers from AWS Artifact.
- AWS SOC 3 Security, Availability & Confidentiality Report, publicly available as a whitepaper.

Using this framework to support your audit preparation

You can use this framework to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to SOC 2 requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the framework. When it's time for an audit, you—or a delegate of your choice—can review the evidence that Audit Manager collected. Either, you can browse the evidence folders in your assessment and choose which evidence you want to include in your assessment report. Or, if you enabled evidence finder, you can search for specific evidence and export it in CSV format, or create an assessment report from your search results. Either way, you can use this assessment report to show that your controls are working as intended.

The framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets
Statement on Standards for Attestations Engagemen t (SSAE) No. 18, Service Organizations Controls (SOC) Report 2	15	46	20

Important

To ensure that this framework collects the intended evidence from AWS Security Hub, make sure that you enabled all standards in Security Hub.
To ensure that this framework collects the intended evidence from AWS Config, make sure that you enable the necessary AWS Config rules. To review the AWS Config rules that are used as data source mappings in this standard framework, download the AuditManager_ConfigDataSourceMappings_SSAE-No.-18-SOC-Report-2.zip file.

The controls in this AWS Audit Manager framework aren't intended to verify if your systems are compliant. Moreover, they can't guarantee that you'll pass an audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

Next steps

For instructions on how to view detailed information about this framework, including the list of standard controls that it contains, see Reviewing a framework in AWS Audit Manager.

For instructions on how to create an assessment using this framework, see Creating an assessment in AWS Audit Manager.

For instructions on how to customize this framework to support your specific requirements, see Making an editable copy of an existing framework in AWS Audit Manager.

Additional resources

- AWS Compliance page for SOC

Supported data source types for automated evidence

When you create a custom control in AWS Audit Manager, you can set up your control to collect automated evidence from the following data source types:

- AWS CloudTrail
- AWS Security Hub
- AWS Config
- AWS API calls

Each data source type offers distinct capabilities for capturing user activity logs, compliance findings, resource configurations, and more.

In this chapter you can learn about each of these automated data source types, and the specific AWS Security Hub controls, AWS Config rules, and AWS API calls that are supported by Audit Manager.

Key points

The following table provides an overview of each automated data source type.

Data source type	Description	Evidence collection frequency	To use this data source type...	When this control is active in an assessment...	Related troubleshooting tips
AWS CloudTrail	Tracks a specific user activity.	Continuous.	Select from the list of supported event names.	Audit Manager filters your CloudTrail logs based on the keyword that you choose. The results are imported as **User activity** evidence.	My assessment isn't collecting user activity evidence from

Data source type	Description	Evidence collection frequency	To use this data source type...	When this control is active in an assessment...	Related troubleshooting tips
					AWS CloudTrail
AWS Config	Captures a snapshot of your resource security posture by reporting findings from AWS Config.	Based on the triggers defined in the AWS Config rule.	Choose a rule type, then select a rule. • For managed rules, select from the list of supported managed rule keywords. • For custom rules, select from the list of your available rules.	Audit Manager gets the findings for this rule directly from AWS Config. The result is imported as **Compliance check** evidence.	My assessment isn't collecting compliance check evidence from AWS Config AWS Config integration issues

Data source type	Description	Evidence collection frequency	To use this data source type...	When this control is active in an assessment...	Related troubleshooting tips
AWS Security Hub	Captures a snapshot of your resource security posture by reporting findings from Security Hub.	Based on the schedule of the Security Hub check.	Select from the list of supported Security Hub control IDs.	Audit Manager gets the result of the security check directly from Security Hub. The result is imported as **Compliance check** evidence.	My assessment isn't collecting compliance check evidence from AWS Security Hub
AWS API calls	Takes a snapshot of your resource configuration directly through an API call to the specified AWS service.	Daily, weekly, or monthly.	Select from the list of supported API calls, then select your preferred frequency.	Audit Manager makes the API call based on the frequency that you specify. The response is imported as **Configuration data** evidence.	My assessment isn't collecting configuration data evidence for an AWS API call

Tip

You can create custom controls that collect evidence using predefined groupings of the above data sources. These data source groupings are known as AWS managed sources. Each AWS managed source represents a common control or a core control that aligns with a common compliance requirement. This gives you an efficient way to map your compliance requirements to a relevant group of AWS data sources. To see the available common controls, see Finding the available controls in AWS Audit Manager.
Alternatively, you can use the four data source types above to define your own custom data sources. This gives you the flexibility to upload manual evidence, or collect automated evidence from a business-specific resource such as a custom AWS Config rule.

Next steps

To learn more about the specific data sources that you can use in your custom controls, see the following pages.

- AWS Config Rules supported by AWS Audit Manager
- AWS Security Hub controls supported by AWS Audit Manager
- AWS API calls supported by AWS Audit Manager
- AWS CloudTrail event names supported by AWS Audit Manager

AWS Config Rules supported by AWS Audit Manager

You can use Audit Manager to capture AWS Config evaluations as evidence for audits. When you create or edit a custom control, you can specify one or more AWS Config rules as a data source mapping for evidence collection. AWS Config performs compliance checks based on these rules, and Audit Manager reports the results as compliance check evidence.

In addition to managed rules, you can also map your custom rules to a control data source.

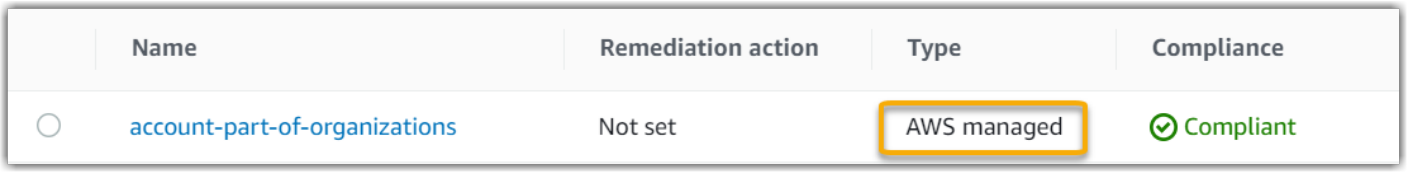
Contents

- Using AWS Config custom rules with Audit Manager
- Additional resources

Key points

- Audit Manager doesn't collect evidence from service-linked AWS Config rules, with the exception of service-linked rules from Conformance Packs and from AWS Organizations.
- Audit Manager doesn't manage AWS Config rules for you. Before you start evidence collection, we recommend that you review your current AWS Config rule parameters. Then, validate those parameters against the requirements of your chosen framework. If needed, you can update a rule's parameters in AWS Config so that it aligns with framework requirements. This will help to ensure that your assessments collect the correct compliance check evidence for that framework.

  For example, suppose that you're creating an assessment for CIS v1.2.0. This framework has a control named Ensure IAM password policy requires a minimum length of 14 or greater. In AWS Config, the iam-password-policy rule has a `MinimumPasswordLength` parameter that checks password length. The default value for this parameter is 14 characters. As a result, the rule aligns with the control requirements. If you aren't using the default parameter value, ensure that the value you're using is equal to or greater than the 14 character requirement from CIS v1.2.0. You can find the default parameter details for each managed rule in the AWS Config documentation.
- If you need to verify if an AWS Config rule is a managed rule or a custom rule, you can do this using the AWS Config console. From the left navigation menu, choose **Rules** and look for the rule in the table. If it's a managed rule, the **Type** column shows **AWS managed**.



Supported AWS Config managed rules

The following AWS Config managed rules are supported by Audit Manager. You can use any of the following managed rule identifier keywords when you set up a data source for a custom control. For more information about any of the managed rules listed below, choose an item from the list or see AWS Config Managed Rules in the *AWS Config User Guide*.

Tip

When you choose a managed rule in the Audit Manager console during custom control creation, make sure that you look for one of the following rule identifier keywords, and not the rule name. For information about the difference between the rule name and rule identifier, and how to find the identifier for a managed rule, see the Troubleshooting section of this user guide.

Supported AWS Config managed rule keywords

- ACCESS_KEYS_ROTATED
- ACCOUNT_PART_OF_ORGANIZATIONS
- ACM_CERTIFICATE_EXPIRATION_CHECK
- ACM_CERTIFICATE_RSA_CHECK
- ALB_DESYNC_MODE_CHECK
- ALB_HTTP_DROP_INVALID_HEADER_ENABLED
- ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK
- ALB_WAF_ENABLED
- API_GW_ASSOCIATED_WITH_WAF
- API_GW_CACHE_ENABLED_AND_ENCRYPTED
- API_GW_ENDPOINT_TYPE_CHECK
- API_GW_EXECUTION_LOGGING_ENABLED
- API_GW_SSL_ENABLED
- API_GW_XRAY_ENABLED
- API_GWV2_ACCESS_LOGS_ENABLED
- API_GWV2_AUTHORIZATION_TYPE_CONFIGURED
- APPROVED_AMIS_BY_ID
- APPROVED_AMIS_BY_TAG
- APPSYNC_ASSOCIATED_WITH_WAF
- APPSYNC_CACHE_ENCRYPTION_AT_REST
- APPSYNC_LOGGING_ENABLED

Supported AWS Config managed rule keywords

- AURORA_LAST_BACKUP_RECOVERY_POINT_CREATED
- AURORA_MYSQL_BACKTRACKING_ENABLED
- AURORA_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- AUTOSCALING_CAPACITY_REBALANCING
- AUTOSCALING_GROUP_ELB_HEALTHCHECK_REQUIRED
- AUTOSCALING_LAUNCH_CONFIG_HOP_LIMIT
- AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED
- AUTOSCALING_LAUNCHCONFIG_REQUIRES_IMDSV2
- AUTOSCALING_LAUNCH_TEMPLATE
- AUTOSCALING_MULTIPLE_AZ
- AUTOSCALING_MULTIPLE_INSTANCE_TYPES
- BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK
- BACKUP_RECOVERY_POINT_ENCRYPTED
- BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
- BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK
- BEANSTALK_ENHANCED_HEALTH_REPORTING_ENABLED
- CLB_DESYNC_MODE_CHECK
- CLB_MULTIPLE_AZ
- CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED
- CLOUD_TRAIL_ENABLED
- CLOUD_TRAIL_ENCRYPTION_ENABLED
- CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED
- CLOUDFORMATION_STACK_DRIFT_DETECTION_CHECK
- CLOUDFORMATION_STACK_NOTIFICATION_CHECK
- CLOUDFRONT_ACCESSLOGS_ENABLED
- CLOUDFRONT_ASSOCIATED_WITH_WAF
- CLOUDFRONT_CUSTOM_SSL_CERTIFICATE
- CLOUDFRONT_DEFAULT_ROOT_OBJECT_CONFIGURED
- CLOUDFRONT_NO_DEPRECATED_SSL_PROTOCOLS

Supported AWS Config managed rule keywords

- CLOUDFRONT_ORIGIN_ACCESS_IDENTITY_ENABLED
- CLOUDFRONT_ORIGIN_FAILOVER_ENABLED
- CLOUDFRONT_S3_ORIGIN_ACCESS_CONTROL_ENABLED
- CLOUDFRONT_S3_ORIGIN_NON_EXISTENT_BUCKET
- CLOUDFRONT_SECURITY_POLICY_CHECK
- CLOUDFRONT_SNI_ENABLED
- CLOUDFRONT_TRAFFIC_TO_ORIGIN_ENCRYPTED
- CLOUDFRONT_VIEWER_POLICY_HTTPS
- CLOUDTRAIL_S3_DATAEVENTS_ENABLED
- CLOUDTRAIL_SECURITY_TRAIL_ENABLED
- CLOUDWATCH_ALARM_ACTION_CHECK
- CLOUDWATCH_ALARM_ACTION_ENABLED_CHECK
- CLOUDWATCH_ALARM_RESOURCE_CHECK
- CLOUDWATCH_ALARM_SETTINGS_CHECK
- CLOUDWATCH_LOG_GROUP_ENCRYPTED
- CMK_BACKING_KEY_ROTATION_ENABLED
- CODEBUILD_PROJECT_ARTIFACT_ENCRYPTION
- CODEBUILD_PROJECT_ENVIRONMENT_PRIVILEGED_CHECK
- CODEBUILD_PROJECT_ENVVAR_AWSCRED_CHECK
- CODEBUILD_PROJECT_LOGGING_ENABLED
- CODEBUILD_PROJECT_S3_LOGS_ENCRYPTED
- CODEBUILD_PROJECT_SOURCE_REPO_URL_CHECK
- CODEDEPLOY_AUTO_ROLLBACK_MONITOR_ENABLED
- CODEDEPLOY_EC2_MINIMUM_HEALTHY_HOSTS_CONFIGURED
- CODEDEPLOY_LAMBDA_ALLATONCE_TRAFFIC_SHIFT_DISABLED
- CODEPIPELINE_DEPLOYMENT_COUNT_CHECK
- CODEPIPELINE_REGION_FANOUT_CHECK
- CUSTOM_SCHEMA_REGISTRY_POLICY_ATTACHED
- CW_LOGGROUP_RETENTION_PERIOD_CHECK

Supported AWS Config managed rule keywords

- DAX_ENCRYPTION_ENABLED
- DB_INSTANCE_BACKUP_ENABLED
- DESIRED_INSTANCE_TENANCY
- DESIRED_INSTANCE_TYPE
- DMS_REPLICATION_NOT_PUBLIC
- DYNAMODB_AUTOSCALING_ENABLED
- DYNAMODB_IN_BACKUP_PLAN
- DYNAMODB_LAST_BACKUP_RECOVERY_POINT_CREATED
- DYNAMODB_PITR_ENABLED
- DYNAMODB_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- DYNAMODB_TABLE_ENCRYPTED_KMS
- DYNAMODB_TABLE_ENCRYPTION_ENABLED
- DYNAMODB_THROUGHPUT_LIMIT_CHECK
- EBS_IN_BACKUP_PLAN
- EBS_LAST_BACKUP_RECOVERY_POINT_CREATED
- EBS_OPTIMIZED_INSTANCE
- EBS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK
- EC2_CLIENT_VPN_NOT_AUTHORIZE_ALL
- EC2_EBS_ENCRYPTION_BY_DEFAULT
- EC2_IMDSV2_CHECK
- EC2_INSTANCE_DETAILED_MONITORING_ENABLED
- EC2_INSTANCE_MANAGED_BY_SSM
- EC2_INSTANCE_MULTIPLE_ENI_CHECK
- EC2_INSTANCE_NO_PUBLIC_IP
- EC2_INSTANCE_PROFILE_ATTACHED
- EC2_LAST_BACKUP_RECOVERY_POINT_CREATED
- EC2_LAUNCH_TEMPLATE_PUBLIC_IP_DISABLED
- EC2_MANAGEDINSTANCE_APPLICATIONS_BLACKLISTED

Supported AWS Config managed rule keywords

- EC2_MANAGEDINSTANCE_APPLICATIONS_REQUIRED
- EC2_MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK
- EC2_MANAGEDINSTANCE_INVENTORY_BLACKLISTED
- EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK
- EC2_MANAGEDINSTANCE_PLATFORM_CHECK
- EC2_NO_AMAZON_KEY_PAIR
- EC2_PARAVIRTUAL_INSTANCE_CHECK
- EC2_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EC2_SECURITY_GROUP_ATTACHED_TO_ENI
- EC2_SECURITY_GROUP_ATTACHED_TO_ENI_PERIODIC
- EC2_STOPPED_INSTANCE
- EC2_TOKEN_HOP_LIMIT_CHECK
- EC2_TRANSIT_GATEWAY_AUTO_VPC_ATTACH_DISABLED
- EC2_VOLUME_INUSE_CHECK
- ECR_PRIVATE_IMAGE_SCANNING_ENABLED
- ECR_PRIVATE_LIFECYCLE_POLICY_CONFIGURED
- ECR_PRIVATE_TAG_IMMUTABILITY_ENABLED
- ECS_AWSVPC_NETWORKING_ENABLED
- ECS_CONTAINER_INSIGHTS_ENABLED
- ECS_CONTAINERS_NONPRIVILEGED
- ECS_CONTAINERS_READONLY_ACCESS
- ECS_FARGATE_LATEST_PLATFORM_VERSION
- ECS_NO_ENVIRONMENT_SECRETS
- ECS_TASK_DEFINITION_LOG_CONFIGURATION
- ECS_TASK_DEFINITION_MEMORY_HARD_LIMIT
- ECS_TASK_DEFINITION_NONROOT_USER
- ECS_TASK_DEFINITION_PID_MODE_CHECK
- ECS_TASK_DEFINITION_USER_FOR_HOST_MODE_CHECK
- EFS_ACCESS_POINT_ENFORCE_ROOT_DIRECTORY

Supported AWS Config managed rule keywords

- EFS_ACCESS_POINT_ENFORCE_USER_IDENTITY
- EFS_ENCRYPTED_CHECK
- EFS_IN_BACKUP_PLAN
- EFS_LAST_BACKUP_RECOVERY_POINT_CREATED
- EFS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EIP_ATTACHED
- EKS_CLUSTER_LOGGING_ENABLED
- EKS_CLUSTER_OLDEST_SUPPORTED_VERSION
- EKS_CLUSTER_SUPPORTED_VERSION
- EKS_ENDPOINT_NO_PUBLIC_ACCESS
- EKS_SECRETS_ENCRYPTED
- ELASTIC_BEANSTALK_LOGS_TO_CLOUDWATCH
- ELASTIC_BEANSTALK_MANAGED_UPDATES_ENABLED
- ELASTICACHE_AUTO_MINOR_VERSION_UPGRADE_CHECK
- ELASTICACHE_RBAC_AUTH_ENABLED
- ELASTICACHE_REDIS_CLUSTER_AUTOMATIC_BACKUP_CHECK
- ELASTICACHE_REPL_GRP_AUTO_FAILOVER_ENABLED
- ELASTICACHE_REPL_GRP_ENCRYPTED_AT_REST
- ELASTICACHE_REPL_GRP_ENCRYPTED_IN_TRANSIT
- ELASTICACHE_REPL_GRP_REDIS_AUTH_ENABLED
- ELASTICACHE_SUBNET_GROUP_CHECK
- ELASTICACHE_SUPPORTED_ENGINE_VERSION
- ELASTICSEARCH_ENCRYPTED_AT_REST
- ELASTICSEARCH_IN_VPC_ONLY
- ELASTICSEARCH_LOGS_TO_CLOUDWATCH
- ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK
- ELB_ACM_CERTIFICATE_REQUIRED
- ELB_CROSS_ZONE_LOAD_BALANCING_ENABLED
- ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK

Supported AWS Config managed rule keywords

- ELB_DELETION_PROTECTION_ENABLED
- ELB_LOGGING_ENABLED
- ELB_PREDEFINED_SECURITY_POLICY_SSL_CHECK
- ELB_TLS_HTTPS_LISTENERS_ONLY
- ELBV2_ACM_CERTIFICATE_REQUIRED
- ELBV2_MULTIPLE_AZ
- EMR_KERBEROS_ENABLED
- EMR_MASTER_NO_PUBLIC_IP
- ENCRYPTED_VOLUMES
- FMS_SHIELD_RESOURCE_POLICY_CHECK
- FMS_WEBACL_RESOURCE_POLICY_CHECK
- FMS_WEBACL_RULEGROUP_ASSOCIATION_CHECK
- FSX_LAST_BACKUP_RECOVERY_POINT_CREATED
- FSX_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- GUARDDUTY_ENABLED_CENTRALIZED
- GUARDDUTY_NON_ARCHIVED_FINDINGS
- IAM_CUSTOMER_POLICY_BLOCKED_KMS_ACTIONS
- IAM_GROUP_HAS_USERS_CHECK
- IAM_INLINE_POLICY_BLOCKED_KMS_ACTIONS
- IAM_NO_INLINE_POLICY_CHECK
- IAM_PASSWORD_POLICY
- IAM_POLICY_BLACKLISTED_CHECK
- IAM_POLICY_IN_USE
- IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS
- IAM_POLICY_NO_STATEMENTS_WITH_FULL_ACCESS
- IAM_ROLE_MANAGED_POLICY_CHECK
- IAM_ROOT_ACCESS_KEY_CHECK
- IAM_USER_GROUP_MEMBERSHIP_CHECK
- IAM_USER_MFA_ENABLED

Supported AWS Config managed rule keywords

- IAM_USER_NO_POLICIES_CHECK
- IAM_USER_UNUSED_CREDENTIALS_CHECK
- INCOMING_SSH_DISABLED
- INSTANCES_IN_VPC
- KINESIS_STREAM_ENCRYPTED
- INTERNET_GATEWAY_AUTHORIZED_VPC_ONLY
- KMS_CMK_NOT_SCHEDULED_FOR_DELETION
- LAMBDA_CONCURRENCY_CHECK
- LAMBDA_DLQ_CHECK
- LAMBDA_FUNCTION_PUBLIC_ACCESS_PROHIBITED
- LAMBDA_FUNCTION_SETTINGS_CHECK
- LAMBDA_INSIDE_VPC
- LAMBDA_VPC_MULTI_AZ_CHECK
- MACIE_STATUS_CHECK
- MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS
- MQ_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED
- MQ_CLOUDWATCH_AUDIT_LOGGING_ENABLED
- MQ_NO_PUBLIC_ACCESS
- MULTI_REGION_CLOUD_TRAIL_ENABLED
- NACL_NO_UNRESTRICTED_SSH_RDP
- NETFW_LOGGING_ENABLED
- NETFW_MULTI_AZ_ENABLED
- NETFW_POLICY_DEFAULT_ACTION_FRAGMENT_PACKETS
- NETFW_POLICY_DEFAULT_ACTION_FULL_PACKETS
- NETFW_POLICY_RULE_GROUP_ASSOCIATED
- NETFW_STATELESS_RULE_GROUP_NOT_EMPTY
- NLB_CROSS_ZONE_LOAD_BALANCING_ENABLED
- NO_UNRESTRICTED_ROUTE_TO_IGW
- OPENSEARCH_ACCESS_CONTROL_ENABLED

Supported AWS Config managed rule keywords

- OPENSEARCH_AUDIT_LOGGING_ENABLED
- OPENSEARCH_DATA_NODE_FAULT_TOLERANCE
- OPENSEARCH_ENCRYPTED_AT_REST
- OPENSEARCH_HTTPS_REQUIRED
- OPENSEARCH_IN_VPC_ONLY
- OPENSEARCH_LOGS_TO_CLOUDWATCH
- OPENSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK
- RDS_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED
- RDS_CLUSTER_DEFAULT_ADMIN_CHECK
- RDS_CLUSTER_DELETION_PROTECTION_ENABLED
- RDS_CLUSTER_IAM_AUTHENTICATION_ENABLED
- RDS_CLUSTER_MULTI_AZ_ENABLED
- RDS_DB_SECURITY_GROUP_NOT_ALLOWED
- RDS_ENHANCED_MONITORING_ENABLED
- RDS_IN_BACKUP_PLAN
- RDS_INSTANCE_DEFAULT_ADMIN_CHECK
- RDS_INSTANCE_DELETION_PROTECTION_ENABLED
- RDS_INSTANCE_IAM_AUTHENTICATION_ENABLED
- RDS_INSTANCE_PUBLIC_ACCESS_CHECK
- RDS_LAST_BACKUP_RECOVERY_POINT_CREATED
- RDS_LOGGING_ENABLED
- RDS_MULTI_AZ_SUPPORT
- RDS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- RDS_SNAPSHOT_ENCRYPTED
- RDS_SNAPSHOTS_PUBLIC_PROHIBITED
- RDS_STORAGE_ENCRYPTED
- REDSHIFT_BACKUP_ENABLED
- REDSHIFT_REQUIRE_TLS_SSL
- REDSHIFT_CLUSTER_CONFIGURATION_CHECK

Supported AWS Config managed rule keywords

- REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK
- REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK
- REDSHIFT_AUDIT_LOGGING_ENABLED
- REDSHIFT_CLUSTER_KMS_ENABLED
- REDSHIFT_DEFAULT_ADMIN_CHECK
- REDSHIFT_DEFAULT_DB_NAME_CHECK
- REDSHIFT_ENHANCED_VPC_ROUTING_ENABLED
- REQUIRED_TAGS
- RESTRICTED_INCOMING_TRAFFIC
- ROOT_ACCOUNT_HARDWARE_MFA_ENABLED
- ROOT_ACCOUNT_MFA_ENABLED
- S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC
- S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS
- S3_BUCKET_ACL_PROHIBITED
- S3_BUCKET_BLACKLISTED_ACTIONS_PROHIBITED
- S3_BUCKET_DEFAULT_LOCK_ENABLED
- S3_BUCKET_LEVEL_PUBLIC_ACCESS_PROHIBITED
- S3_BUCKET_LOGGING_ENABLED
- S3_BUCKET_POLICY_GRANTEE_CHECK
- S3_BUCKET_POLICY_NOT_MORE_PERMISSIVE
- S3_BUCKET_PUBLIC_READ_PROHIBITED
- S3_BUCKET_PUBLIC_WRITE_PROHIBITED
- S3_BUCKET_REPLICATION_ENABLED
- S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED
- S3_BUCKET_SSL_REQUESTS_ONLY
- S3_BUCKET_VERSIONING_ENABLED
- S3_DEFAULT_ENCRYPTION_KMS
- S3_EVENT_NOTIFICATIONS_ENABLED
- S3_LAST_BACKUP_RECOVERY_POINT_CREATED

Supported AWS Config managed rule keywords

- S3_LIFECYCLE_POLICY_CHECK
- S3_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- S3_VERSION_LIFECYCLE_POLICY_CHECK
- SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED
- SAGEMAKER_NOTEBOOK_INSTANCE_INSIDE_VPC
- SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED
- SAGEMAKER_NOTEBOOK_INSTANCE_ROOT_ACCESS_CHECK
- SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS
- SECRETSMANAGER_ROTATION_ENABLED_CHECK
- SECRETSMANAGER_SCHEDULED_ROTATION_SUCCESS_CHECK
- SECRETSMANAGER_SECRET_PERIODIC_ROTATION
- SECRETSMANAGER_SECRET_UNUSED
- SECRETSMANAGER_USING_CMK
- SECURITY_ACCOUNT_INFORMATION_PROVIDED
- SECURITYHUB_ENABLED
- SERVICE_VPC_ENDPOINT_ENABLED
- SES_MALWARE_SCANNING_ENABLED
- SHIELD_ADVANCED_ENABLED_AUTORENEW
- SHIELD_DRT_ACCESS
- SNS_ENCRYPTED_KMS
- SNS_TOPIC_MESSAGE_DELIVERY_NOTIFICATION_ENABLED
- SSM_DOCUMENT_NOT_PUBLIC
- STEP_FUNCTIONS_STATE_MACHINE_LOGGING_ENABLED
- STORAGEGATEWAY_LAST_BACKUP_RECOVERY_POINT_CREATED
- STORAGEGATEWAY_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED
- VIRTUALMACHINE_LAST_BACKUP_RECOVERY_POINT_CREATED
- VIRTUALMACHINE_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- VPC_DEFAULT_SECURITY_GROUP_CLOSED

Supported AWS Config managed rule keywords

- VPC_FLOW_LOGS_ENABLED
- VPC_NETWORK_ACL_UNUSED_CHECK
- VPC_PEERING_DNS_RESOLUTION_CHECK
- VPC_SG_OPEN_ONLY_TO_AUTHORIZED_PORTS
- VPC_VPN_2_TUNNELS_UP
- WAF_CLASSIC_LOGGING_ENABLED
- WAF_GLOBAL_RULEGROUP_NOT_EMPTY
- WAF_GLOBAL_RULE_NOT_EMPTY
- WAF_GLOBAL_WEBACL_NOT_EMPTY
- WAF_REGIONAL_RULEGROUP_NOT_EMPTY
- WAF_REGIONAL_RULE_NOT_EMPTY
- WAF_REGIONAL_WEBACL_NOT_EMPTY
- WAFV2_LOGGING_ENABLED
- WAFV2_RULEGROUP_NOT_EMPTY
- WAFV2_WEBACL_NOT_EMPTY

Using AWS Config custom rules with Audit Manager

You can use AWS Config custom rules as a data source for audit reporting. When a control has a data source that's mapped to an AWS Config rule, Audit Manager adds the evaluation that was created by the AWS Config rule.

The custom rules that you can use depend on the AWS account that you sign in to Audit Manager with. If you can access a custom rule in AWS Config, you can use it as a data source mapping in Audit Manager.

- **For individual AWS accounts** – You can use any of the custom rules that you created with your account.
- **For accounts that are part of an organization** – Either, you can use any of your member-level custom rules. Or, you can use any of the organization-level custom rules that are available to you in AWS Config.

After you map your custom rules as a data source for a control, you can add that control to a custom framework in Audit Manager.

Additional resources

- To find help with issues for this data source type, see My assessment isn't collecting compliance check evidence from AWS Config and AWS Config integration issues.
- To create a custom control using this data source type, see Creating a custom control in AWS Audit Manager.
- To create a custom framework that uses your custom control, see Creating a custom framework in AWS Audit Manager.
- To add your custom control to an existing custom framework, see Editing a custom framework in AWS Audit Manager.
- To create a custom rule in AWS Config, see Developing a custom rule for AWS Config in the *AWS Config Developer Guide*.

AWS Security Hub controls supported by AWS Audit Manager

You can use Audit Manager to capture Security Hub findings as evidence for audits. When you create or edit a custom control, you can specify one or more Security Hub controls as a data source mapping for evidence collection. Security Hub performs compliance checks based on these controls, and Audit Manager reports the results as compliance check evidence.

Contents

Key points

- Audit Manager doesn't collect evidence from service-linked AWS Config rules that are created by Security Hub.
- On November 9, 2022, Security Hub launched automated security checks aligned to the Center for Internet Security's (CIS) AWS Foundations Benchmark version 1.4.0 requirements, Level 1 and

2 (CIS v1.4.0). In Security Hub, the CIS v1.4.0 standard is supported in addition to the CIS v1.2.0 standard.

- We recommend that you turn on the consolidated control findings setting in Security Hub if it's not turned on already. If you enable Security Hub on or after February 23, 2023, this setting is turned *on* by default.

  When consolidated findings is enabled, Security Hub produces a single finding for each security check (even when the same check applies to multiple standards). Each Security Hub finding is collected as one unique resource assessment in Audit Manager. As a result, consolidated findings results in a decrease of the total unique resource assessments that Audit Manager performs for Security Hub findings. For this reason, using consolidated findings can often result in a reduction in your Audit Manager usages costs, without sacrificing evidence quality and availability. For more information about pricing, see AWS Audit Manager Pricing.

Examples of evidence when consolidated findings is turned on or off

The following examples show a comparison of how Audit Manager collects and presents evidence depending on your Security Hub settings.

When consolidated findings is turned on

Let's say that you have enabled the following three security standards in Security Hub: AWS FSBP, PCI DSS, and CIS Benchmark v1.2.0.

- All three of these standards use the same control (IAM.4) with the same underlying AWS Config rule (iam-root-access-key-check).
- Because the consolidated findings setting is **turned on**, Security Hub generates one single finding for this control.
- Security Hub sends the consolidated finding to Audit Manager for this control.
- The consolidated finding counts as one unique resource assessment in Audit Manager. As a result, one single piece of evidence is added to your assessment.

Here's an example of how that evidence might look:

```
{
    "SchemaVersion": "2018-10-08",
```

```
    "Id": "arn:aws:securityhub:us-west-2:111122223333:security-control/IAM.4/
finding/09876543-p0o9-i8u7-y6t5-098765432109",
    "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/securityhub",
    "ProductName": "Security Hub",
    "CompanyName": "AWS",
    "Region": "us-west-2",
    "GeneratorId": "security-control/IAM.4",
    "AwsAccountId": "111122223333",
    "Types": [
        "Software and Configuration Checks/Industry and Regulatory Standards"
    ],
    "FirstObservedAt": "2023-10-25T11:32:24.861Z",
    "LastObservedAt": "2023-11-02T11:59:19.546Z",
    "CreatedAt": "2023-10-25T11:32:24.861Z",
    "UpdatedAt": "2023-11-02T11:59:15.127Z",
    "Severity": {
        "Label": "INFORMATIONAL",
        "Normalized": 0,
        "Original": "INFORMATIONAL"
    },
    "Title": "IAM root user access key should not exist",
    "Description": "This AWS control checks whether the root user access key is
 available.",
    "Remediation": {
        "Recommendation": {
            "Text": "For information on how to correct this issue, consult the AWS
 Security Hub controls documentation.",
            "Url": "https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
        }
    },
    "ProductFields": {
        "RelatedAWSResources:0/name": "securityhub-iam-root-access-key-
check-000270f5",
        "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
        "aws/securityhub/ProductName": "Security Hub",
        "aws/securityhub/CompanyName": "AWS",
        "Resources:0/Id": "arn:aws:iam::111122223333:root",
        "aws/securityhub/FindingId": "arn:aws:securityhub:us-west-2::product/aws/
securityhub/arn:aws:securityhub:us-west-2:111122223333:security-control/IAM.4/
finding/09876543-p0o9-i8u7-y6t5-098765432109"
    },
    "Resources": [{
        "Type": "AwsAccount",
```

```
        "Id": "AWS::::Account:111122223333",
        "Partition": "aws",
        "Region": "us-west-2"
    }],
    "Compliance": {
        "Status": "PASSED",
        "RelatedRequirements": [
            "CIS AWS Foundations Benchmark v1.2.0/1.12"
        ],
        "SecurityControlId": "IAM.4",
        "AssociatedStandards": [{
                "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"
            },
            {
                "StandardsId": "standards/aws-foundational-security-best-practices/
v/1.0.0"
            }
        ]
    },
    "WorkflowState": "NEW",
    "Workflow": {
        "Status": "RESOLVED"
    },
    "RecordState": "ACTIVE",
    "FindingProviderFields": {
        "Severity": {
            "Label": "INFORMATIONAL",
            "Original": "INFORMATIONAL"
        },
        "Types": [
            "Software and Configuration Checks/Industry and Regulatory Standards"
        ]
    },
    "ProcessedAt": "2023-11-02T11:59:20.980Z"
}
```


When consolidated findings is turned off

Let's say that you have enabled the following three security standards in Security Hub: AWS FSBP, PCI DSS, and CIS Benchmark v1.2.0.

- All three of these standards use the same control (IAM.4) with the same underlying AWS Config rule (iam-root-access-key-check).

- Because the consolidated findings setting is **turned off**, Security Hub generates a separate finding per security check for each enabled standard (in this case, three findings).
- Security Hub sends three separate standard-specific findings to Audit Manager for this control.
- The three findings count as three unique resource assessments in Audit Manager. As a result, three separate pieces of evidence are added to your assessment.

Here's an example of how that evidence might look. Note that in this example, each of the following three payloads has the same security control ID (*SecurityControlId":"IAM.4"*). For this reason, the assessment control that collects this evidence in Audit Manager (IAM.4) receives three separate pieces of evidence when the following findings come in from Security Hub.

Evidence for IAM.4 (FSBP)


```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
     "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/b5e68d5d-43c3-46c8-902d-51cb0d4da568"
  ],
  "detail":{
     "findings":[
        {
           "SchemaVersion":"2018-10-08",
           "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/aws-
foundational-security-best-practices/v/1.0.0/IAM.4/finding/8e2e05a2-4d50-4c2e-
a78f-3cbe9402d17d",
           "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
           "ProductName":"Security Hub",
           "CompanyName":"AWS",
           "Region":"us-west-2",
           "GeneratorId":"aws-foundational-security-best-practices/v/1.0.0/IAM.4",
           "AwsAccountId":"111122223333",
```

```
            "Types":[
               "Software and Configuration Checks/Industry and Regulatory Standards/
AWS-Foundational-Security-Best-Practices"
            ],
            "FirstObservedAt":"2020-10-05T19:18:47.848Z",
            "LastObservedAt":"2023-11-01T14:12:04.106Z",
            "CreatedAt":"2020-10-05T19:18:47.848Z",
            "UpdatedAt":"2023-11-01T14:11:53.720Z",
            "Severity":{
               "Product":0,
               "Label":"INFORMATIONAL",
               "Normalized":0,
               "Original":"INFORMATIONAL"
            },
            "Title":"IAM.4 IAM root user access key should not exist",
            "Description":"This AWS control checks whether the root user access key
 is available.",
            "Remediation":{
               "Recommendation":{
                  "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
                  "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
               }
            },
            "ProductFields":{
               "StandardsArn":"arn:aws:securityhub:::standards/aws-foundational-
security-best-practices/v/1.0.0",
               "StandardsSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0",
               "ControlId":"IAM.4",
               "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
               "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
               "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
               "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/aws-foundational-security-best-practices/v/1.0.0/IAM.4",
               "aws/securityhub/ProductName":"Security Hub",
               "aws/securityhub/CompanyName":"AWS",
               "Resources:0/Id":"arn:aws:iam::111122223333:root",
               "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/aws-
```

```
foundational-security-best-practices/v/1.0.0/IAM.4/finding/8e2e05a2-4d50-4c2e-
a78f-3cbe9402d17d"
            },
            "Resources":[
               {
                  "Type":"AwsAccount",
                  "Id":"AWS::::Account:111122223333",
                  "Partition":"aws",
                  "Region":"us-west-2"
               }
            ],
            "Compliance":{
               "Status":"PASSED",
               "SecurityControlId":"IAM.4",
               "AssociatedStandards":[
                  {
                     "StandardsId":"standards/aws-foundational-security-best-
practices/v/1.0.0"
                  }
               ]
            },
            "WorkflowState":"NEW",
            "Workflow":{
               "Status":"RESOLVED"
            },
            "RecordState":"ACTIVE",
            "FindingProviderFields":{
               "Severity":{
                  "Label":"INFORMATIONAL",
                  "Original":"INFORMATIONAL"
               },
               "Types":[
                  "Software and Configuration Checks/Industry and Regulatory
 Standards/AWS-Foundational-Security-Best-Practices"
               ]
            },
            "ProcessedAt":"2023-11-01T14:12:07.395Z"
         }
      ]
   }
}
```

Evidence for IAM.4 (CIS 1.2)


```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
     "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
  ],
  "detail":{
     "findings":[
        {
           "SchemaVersion":"2018-10-08",
           "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/cis-aws-
foundations-benchmark/v/1.2.0/1.12/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23",
           "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
           "ProductName":"Security Hub",
           "CompanyName":"AWS",
           "Region":"us-west-2",
           "GeneratorId":"arn:aws:securityhub:::ruleset/cis-aws-foundations-
benchmark/v/1.2.0/rule/1.12",
           "AwsAccountId":"111122223333",
           "Types":[
              "Software and Configuration Checks/Industry and Regulatory Standards/
CIS AWS Foundations Benchmark"
           ],
           "FirstObservedAt":"2020-10-05T19:18:47.775Z",
           "LastObservedAt":"2023-11-01T14:12:07.989Z",
           "CreatedAt":"2020-10-05T19:18:47.775Z",
           "UpdatedAt":"2023-11-01T14:11:53.720Z",
           "Severity":{
              "Product":0,
              "Label":"INFORMATIONAL",
              "Normalized":0,
              "Original":"INFORMATIONAL"
           },
           "Title":"1.12 Ensure no root user access key exists",
```

```
            "Description":"The root user is the most privileged user in an AWS
 account. AWS Access Keys provide programmatic access to a given AWS account. It is
 recommended that all access keys associated with the root user be removed.",
            "Remediation":{
               "Recommendation":{
                  "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
                  "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
               }
            },
            "ProductFields":{
               "StandardsGuideArn":"arn:aws:securityhub:::ruleset/cis-aws-
foundations-benchmark/v/1.2.0",
               "StandardsGuideSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/cis-aws-foundations-benchmark/v/1.2.0",
               "RuleId":"1.12",
               "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
               "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
               "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
               "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/cis-aws-foundations-benchmark/v/1.2.0/1.12",
               "aws/securityhub/ProductName":"Security Hub",
               "aws/securityhub/CompanyName":"AWS",
               "Resources:0/Id":"arn:aws:iam::111122223333:root",
               "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/cis-aws-
foundations-benchmark/v/1.2.0/1.12/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
            },
            "Resources":[
               {
                  "Type":"AwsAccount",
                  "Id":"AWS::::Account:111122223333",
                  "Partition":"aws",
                  "Region":"us-west-2"
               }
            ],
            "Compliance":{
               "Status":"PASSED",
               "SecurityControlId":"IAM.4",
               "AssociatedStandards":[
                  {
```

```
                  "StandardsId":"ruleset/cis-aws-foundations-benchmark/v/1.2.0"
               }
            ]
         },
         "WorkflowState":"NEW",
         "Workflow":{
            "Status":"RESOLVED"
         },
         "RecordState":"ACTIVE",
         "FindingProviderFields":{
            "Severity":{
               "Label":"INFORMATIONAL",
               "Original":"INFORMATIONAL"
            },
            "Types":[
               "Software and Configuration Checks/Industry and Regulatory
 Standards/CIS AWS Foundations Benchmark"
            ]
         },
         "ProcessedAt":"2023-11-01T14:12:13.436Z"
      }
   ]
  }
}
```


Evidence for PCI.IAM.1 (PCI DSS)


```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
     "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
  ],
  "detail":{
     "findings":[
        {
```

```
            "SchemaVersion":"2018-10-08",
            "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/pci-dss/
v/3.2.1/PCI.IAM.1/finding/3c75f651-6e2e-44f4-8e22-297d5c2d0c8b",
            "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
            "ProductName":"Security Hub",
            "CompanyName":"AWS",
            "Region":"us-west-2",
            "GeneratorId":"pci-dss/v/3.2.1/PCI.IAM.1",
            "AwsAccountId":"111122223333",
            "Types":[
               "Software and Configuration Checks/Industry and Regulatory Standards/
PCI-DSS"
            ],
            "FirstObservedAt":"2020-10-05T19:18:47.788Z",
            "LastObservedAt":"2023-11-01T14:12:02.413Z",
            "CreatedAt":"2020-10-05T19:18:47.788Z",
            "UpdatedAt":"2023-11-01T14:11:53.720Z",
            "Severity":{
               "Product":0,
               "Label":"INFORMATIONAL",
               "Normalized":0,
               "Original":"INFORMATIONAL"
            },
            "Title":"PCI.IAM.1 IAM root user access key should not exist",
            "Description":"This AWS control checks whether the root user access key
 is available.",
            "Remediation":{
               "Recommendation":{
                  "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
                  "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
               }
            },
            "ProductFields":{
               "StandardsArn":"arn:aws:securityhub:::standards/pci-dss/v/3.2.1",
               "StandardsSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/pci-dss/v/3.2.1",
               "ControlId":"PCI.IAM.1",
               "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
               "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
               "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
```

```
              "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/pci-dss/v/3.2.1/PCI.IAM.1",
              "aws/securityhub/ProductName":"Security Hub",
              "aws/securityhub/CompanyName":"AWS",
              "Resources:0/Id":"arn:aws:iam::111122223333:root",
              "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/pci-dss/
v/3.2.1/PCI.IAM.1/finding/3c75f651-6e2e-44f4-8e22-297d5c2d0c8b"
           },
           "Resources":[
              {
                 "Type":"AwsAccount",
                 "Id":"AWS::::Account:111122223333",
                 "Partition":"aws",
                 "Region":"us-west-2"
              }
           ],
           "Compliance":{
              "Status":"PASSED",
              "RelatedRequirements":[
                 "PCI DSS 2.1",
                 "PCI DSS 2.2",
                 "PCI DSS 7.2.1"
              ],
              "SecurityControlId":"IAM.4",
              "AssociatedStandards":[
                 {
                    "StandardsId":"standards/pci-dss/v/3.2.1"
                 }
              ]
           },
           "WorkflowState":"NEW",
           "Workflow":{
              "Status":"RESOLVED"
           },
           "RecordState":"ACTIVE",
           "FindingProviderFields":{
              "Severity":{
                 "Label":"INFORMATIONAL",
                 "Original":"INFORMATIONAL"
              },
              "Types":[
                 "Software and Configuration Checks/Industry and Regulatory
 Standards/PCI-DSS"
```

```
            ]
          },
          "ProcessedAt":"2023-11-01T14:12:05.950Z"
        }
      ]
    }
}
```

Supported Security Hub controls

The following Security Hub controls are currently supported by Audit Manager. You can use any of the following standard-specific control ID keywords when you set up a data source for a custom control.

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
CIS v1.2.0	1.2	IAM.5
CIS v1.2.0	1.3	IAM.8
CIS v1.2.0	1.4	IAM.3
CIS v1.2.0	1.5	IAM.11
CIS v1.2.0	1.6	IAM.12
CIS v1.2.0	1.7	IAM.13
CIS v1.2.0	1.8	IAM.14
CIS v1.2.0	1.9	IAM.15
CIS v1.2.0	1.10	IAM.16

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
CIS v1.2.0	1.11	IAM.17
CIS v1.2.0	1.12	IAM.4
CIS v1.2.0	1.13	IAM.9
CIS v1.2.0	1.14	IAM.6
CIS v1.2.0	1.16	IAM.2
CIS v1.2.0	1.20	IAM.18
CIS v1.2.0	1.22	IAM.1
CIS v1.2.0	2.1	CloudTrail.1
CIS v1.2.0	2.2	CloudTrail.4
CIS v1.2.0	2.3	CloudTrail.6
CIS v1.2.0	2.4	CloudTrail.5
CIS v1.2.0	2.5	Config.1
CIS v1.2.0	2.6	CloudTrail.7
CIS v1.2.0	2.7	CloudTrail.2
CIS v1.2.0	2.8	KMS.4
CIS v1.2.0	2.9	EC2.6
CIS v1.2.0	3.1	CloudWatch.2

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
CIS v1.2.0	3.2	CloudWatch.3
CIS v1.2.0	3.3	CloudWatch.1
CIS v1.2.0	3.4	CloudWatch.4
CIS v1.2.0	3.5	CloudWatch.5
CIS v1.2.0	3.6	CloudWatch.6
CIS v1.2.0	3.7	CloudWatch.7
CIS v1.2.0	3.8	CloudWatch.8
CIS v1.2.0	3.9	CloudWatch.9
CIS v1.2.0	3.10	CloudWatch.10
CIS v1.2.0	3.11	CloudWatch.11
CIS v1.2.0	3.12	CloudWatch.12
CIS v1.2.0	3.13	CloudWatch.13
CIS v1.2.0	3.14	CloudWatch.14
CIS v1.2.0	4.1	EC2.13
CIS v1.2.0	4.2	EC2.14
CIS v1.2.0	4.3	EC2.2

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
PCI DSS	PCI.AutoScaling.1	AutoScaling.1
PCI DSS	PCI.CloudTrail.1	CloudTrail.1
PCI DSS	PCI.CloudTrail.2	CloudTrail.2
PCI DSS	PCI.CloudTrail.3	CloudTrail.3
PCI DSS	PCI.CloudTrail.4	CloudTrail.4
PCI DSS	PCI.CodeBuild.1	CodeBuild.1
PCI DSS	PCI.CodeBuild.2	CodeBuild.2
PCI DSS	PCI.Config.1	Config.1
PCI DSS	PCI.CW.1	CloudWatch.1
PCI DSS	PCI.DMS.1	DMS.1
PCI DSS	PCI.EC2.1	EC2.1
PCI DSS	PCI.EC2.2	EC2.2
PCI DSS	PCI.EC2.3	EC2.3
PCI DSS	PCI.EC2.4	EC2.12
PCI DSS	PCI.EC2.5	EC2.13
PCI DSS	PCI.EC2.6	EC2.6

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
PCI DSS	PCI.ELBv2.1	ELB.1
PCI DSS	PCI.ES.1	ES.1
PCI DSS	PCI.ES.2	ES.2
PCI DSS	PCI.GuardDuty.1	GuardDuty.1
PCI DSS	PCI.IAM.1	IAM.1
PCI DSS	PCI.IAM.2	IAM.2
PCI DSS	PCI.IAM.3	IAM.3
PCI DSS	PCI.IAM.4	IAM.4
PCI DSS	PCI.IAM.5	IAM.9
PCI DSS	PCI.IAM.6	IAM.6
PCI DSS	PCI.IAM.7	PCI.IAM.7
PCI DSS	PCI.IAM.8	PCI.IAM8.
PCI DSS	PCI.KMS.1	PCI.KMS.4
PCI DSS	PCI.Lambda.1	Lambda.1
PCI DSS	PCI.Lambda.2	Lambda.3
PCI DSS	PCI.Opensearch.1	Opensearch.1

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
PCI DSS	PCI.Opensearch.2	Opensearch.2
PCI DSS	PCI.RDS.1	RDS.1
PCI DSS	PCI.RDS.2	RDS.2
PCI DSS	PCI.Redshift.1	Redshift.1
PCI DSS	PCI.S3.1	S3.1
PCI DSS	PCI.S3.2	S3.2
PCI DSS	PCI.S3.3	S3.3
PCI DSS	PCI.S3.4	S3.4
PCI DSS	PCI.S3.5	S3.5
PCI DSS	PCI.S3.6	S3.1
PCI DSS	PCI.SageMaker.1	SageMaker.1
PCI DSS	PCI.SSM.1	SSM.1
PCI DSS	PCI.SSM.2	SSM.2
PCI DSS	PCI.SSM.3	SSM.3
AWS Foundational Security Best Practices	Account.1	Account.1

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	Account.2	Account.2
AWS Foundational Security Best Practices	ACM.1	ACM.1
AWS Foundational Security Best Practices	ACM.2	ACM.2
AWS Foundational Security Best Practices	APIGateway.1	APIGateway.1
AWS Foundational Security Best Practices	APIGateway.2	APIGateway.2
AWS Foundational Security Best Practices	APIGateway.3	APIGateway.3
AWS Foundational Security Best Practices	APIGateway.4	APIGateway.4
AWS Foundational Security Best Practices	APIGateway.5	APIGateway.5
AWS Foundational Security Best Practices	APIGateway.8	APIGateway.8
AWS Foundational Security Best Practices	APIGateway.9	APIGateway.9

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	AppSync.2	AppSync.2
AWS Foundational Security Best Practices	AppSync.5	AppSync.5
AWS Foundational Security Best Practices	Athena.1	Athena.1
AWS Foundational Security Best Practices	AutoScaling.1	AutoScaling.1
AWS Foundational Security Best Practices	AutoScaling.2	AutoScaling.2
AWS Foundational Security Best Practices	AutoScaling.3	AutoScaling.3
AWS Foundational Security Best Practices	AutoScaling.4	AutoScaling.4
AWS Foundational Security Best Practices	Autoscaling.5	Autoscaling.5
AWS Foundational Security Best Practices	AutoScaling.6	AutoScaling.6
AWS Foundational Security Best Practices	AutoScaling.9	AutoScaling.9

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	Backup.1	Backup.1
AWS Foundational Security Best Practices	CloudFormation.1	CloudFormation.1
AWS Foundational Security Best Practices	CloudFront.1	CloudFront.1
AWS Foundational Security Best Practices	CloudFront.2	CloudFront.2
AWS Foundational Security Best Practices	CloudFront.3	CloudFront.3
AWS Foundational Security Best Practices	CloudFront.4	CloudFront.4
AWS Foundational Security Best Practices	CloudFront.5	CloudFront.5
AWS Foundational Security Best Practices	CloudFront.6	CloudFront.6
AWS Foundational Security Best Practices	CloudFront.7	CloudFront.7
AWS Foundational Security Best Practices	CloudFront.8	CloudFront.8

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	CloudFront.9	CloudFront.9
AWS Foundational Security Best Practices	CloudFront.10	CloudFront.10
AWS Foundational Security Best Practices	CloudFront.12	CloudFront.12
AWS Foundational Security Best Practices	CloudFront.13	CloudFront.13
AWS Foundational Security Best Practices	CloudTrail.1	CloudTrail.1
AWS Foundational Security Best Practices	CloudTrail.2	CloudTrail.2
AWS Foundational Security Best Practices	CloudTrail.3	CloudTrail.3
AWS Foundational Security Best Practices	CloudTrail.4	CloudTrail.4
AWS Foundational Security Best Practices	CloudTrail.5	CloudTrail.5
AWS Foundational Security Best Practices	CloudTrail.6	CloudTrail.6

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	CloudTrail.7	CloudTrail.7
AWS Foundational Security Best Practices	CloudWatch.1	CloudWatch.1
AWS Foundational Security Best Practices	CloudWatch.2	CloudWatch.2
AWS Foundational Security Best Practices	CloudWatch.3	CloudWatch.3
AWS Foundational Security Best Practices	CloudWatch.4	CloudWatch.4
AWS Foundational Security Best Practices	CloudWatch.5	CloudWatch.5
AWS Foundational Security Best Practices	CloudWatch.6	CloudWatch.6
AWS Foundational Security Best Practices	CloudWatch.7	CloudWatch.7
AWS Foundational Security Best Practices	CloudWatch.8	CloudWatch.8
AWS Foundational Security Best Practices	CloudWatch.9	CloudWatch.9

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	CloudWatch.10	CloudWatch.10
AWS Foundational Security Best Practices	CloudWatch.11	CloudWatch.11
AWS Foundational Security Best Practices	CloudWatch.12	CloudWatch.12
AWS Foundational Security Best Practices	CloudWatch.13	CloudWatch.13
AWS Foundational Security Best Practices	CloudWatch.14	CloudWatch.14
AWS Foundational Security Best Practices	CloudWatch.15	CloudWatch.15
AWS Foundational Security Best Practices	CloudWatch.16	CloudWatch.16
AWS Foundational Security Best Practices	CloudWatch.17	CloudWatch.17
AWS Foundational Security Best Practices	CodeBuild.1	CodeBuild.1
AWS Foundational Security Best Practices	CodeBuild.2	CodeBuild.2

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	CodeBuild.3	CodeBuild.3
AWS Foundational Security Best Practices	CodeBuild.4	CodeBuild.4
AWS Foundational Security Best Practices	CodeBuild.5	CodeBuild.5
AWS Foundational Security Best Practices	Config.1	Config.1
AWS Foundational Security Best Practices	DMS.1	DMS.1
AWS Foundational Security Best Practices	DMS.6	DMS.6
AWS Foundational Security Best Practices	DMS.7	DMS.7
AWS Foundational Security Best Practices	DMS.8	DMS.8
AWS Foundational Security Best Practices	DMS.9	DMS.9
AWS Foundational Security Best Practices	DocumentDB.1	DocumentDB.1

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	DocumentDB.2	DocumentDB.2
AWS Foundational Security Best Practices	DocumentDB.3	DocumentDB.3
AWS Foundational Security Best Practices	DocumentDB.4	DocumentDB.4
AWS Foundational Security Best Practices	DocumentDB.5	DocumentDB.5
AWS Foundational Security Best Practices	DynamoDB.1	DynamoDB.1
AWS Foundational Security Best Practices	DynamoDB.2	DynamoDB.2
AWS Foundational Security Best Practices	DynamoDB.3	DynamoDB.3
AWS Foundational Security Best Practices	DynamoDB.4	DynamoDB.4
AWS Foundational Security Best Practices	DynamoDB.6	DynamoDB.6
AWS Foundational Security Best Practices	EC2.1	EC2.1

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	EC2.2	EC2.2
AWS Foundational Security Best Practices	EC2.3	EC2.3
AWS Foundational Security Best Practices	EC2.4	EC2.4
AWS Foundational Security Best Practices	EC2.6	EC2.6
AWS Foundational Security Best Practices	EC2.7	EC2.7
AWS Foundational Security Best Practices	EC2.8	EC2.8
AWS Foundational Security Best Practices	EC2.9	EC2.9
AWS Foundational Security Best Practices	EC2.10	EC2.10
AWS Foundational Security Best Practices	EC2.12	EC2.12
AWS Foundational Security Best Practices	EC2.13	EC2.13

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	EC2.14	EC2.14
AWS Foundational Security Best Practices	EC2.15	EC2.15
AWS Foundational Security Best Practices	EC2.16	EC2.16
AWS Foundational Security Best Practices	EC2.17	EC2.17
AWS Foundational Security Best Practices	EC2.18	EC2.18
AWS Foundational Security Best Practices	EC2.19	EC2.19
AWS Foundational Security Best Practices	EC2.20	EC2.20
AWS Foundational Security Best Practices	EC2.21	EC2.21
AWS Foundational Security Best Practices	EC2.22	EC2.22
AWS Foundational Security Best Practices	EC2.23	EC2.23

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	EC2.24	EC2.24
AWS Foundational Security Best Practices	EC2.25	EC2.25
AWS Foundational Security Best Practices	EC2.28	EC2.28
AWS Foundational Security Best Practices	EC2.51	EC2.51
AWS Foundational Security Best Practices	ECR.1	ECR.1
AWS Foundational Security Best Practices	ECR.2	ECR.2
AWS Foundational Security Best Practices	ECR.3	ECR.3
AWS Foundational Security Best Practices	ECS.1	ECS.1
AWS Foundational Security Best Practices	ECS.2	ECS.2
AWS Foundational Security Best Practices	ECS.3	ECS.3

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	ECS.4	ECS.4
AWS Foundational Security Best Practices	ECS.5	ECS.5
AWS Foundational Security Best Practices	ECS.8	ECS.8
AWS Foundational Security Best Practices	ECS.9	ECS.9
AWS Foundational Security Best Practices	ECS.10	ECS.10
AWS Foundational Security Best Practices	ECS.12	ECS.12
AWS Foundational Security Best Practices	EFS.1	EFS.1
AWS Foundational Security Best Practices	EFS.2	EFS.2
AWS Foundational Security Best Practices	EFS.3	EFS.3
AWS Foundational Security Best Practices	EFS.4	EFS.4

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	EKS.1	EKS.1
AWS Foundational Security Best Practices	EKS.2	EKS.2
AWS Foundational Security Best Practices	EKS.8	EKS.8
AWS Foundational Security Best Practices	ElastiCache.1	ElastiCache.1
AWS Foundational Security Best Practices	ElastiCache.2	ElastiCache.2
AWS Foundational Security Best Practices	ElastiCache.3	ElastiCache.3
AWS Foundational Security Best Practices	ElastiCache.4	ElastiCache.4
AWS Foundational Security Best Practices	ElastiCache.5	ElastiCache.5
AWS Foundational Security Best Practices	ElastiCache.6	ElastiCache.6
AWS Foundational Security Best Practices	ElastiCache.7	ElastiCache.7

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	ElasticBeanstalk.1	ElasticBeanstalk.1
AWS Foundational Security Best Practices	ElasticBeanstalk.2	ElasticBeanstalk.2
AWS Foundational Security Best Practices	ElasticBeanstalk.3	ElasticBeanstalk.3
AWS Foundational Security Best Practices	ELB.1	ELB.1
AWS Foundational Security Best Practices	ELB.2	ELB.2
AWS Foundational Security Best Practices	ELB.3	ELB.3
AWS Foundational Security Best Practices	ELB.4	ELB.4
AWS Foundational Security Best Practices	ELB.5	ELB.5
AWS Foundational Security Best Practices	ELB.6	ELB.6
AWS Foundational Security Best Practices	ELB.7	ELB.7

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	ELB.8	ELB.8
AWS Foundational Security Best Practices	ELB.9	ELB.9
AWS Foundational Security Best Practices	ELB.10	ELB.10
AWS Foundational Security Best Practices	ELB.12	ELB.12
AWS Foundational Security Best Practices	ELB.13	ELB.13
AWS Foundational Security Best Practices	ELB.14	ELB.14
AWS Foundational Security Best Practices	ELB.16	ELB.16
AWS Foundational Security Best Practices	ELBv2.1	ELB.1
AWS Foundational Security Best Practices	EMR.1	EMR.1
AWS Foundational Security Best Practices	EMR.2	EMR.2

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	ES.1	ES.1
AWS Foundational Security Best Practices	ES.2	ES.2
AWS Foundational Security Best Practices	ES.3	ES.3
AWS Foundational Security Best Practices	ES.4	ES.4
AWS Foundational Security Best Practices	ES.5	ES.5
AWS Foundational Security Best Practices	ES.6	ES.6
AWS Foundational Security Best Practices	ES.7	ES.7
AWS Foundational Security Best Practices	ES.8	ES.8
AWS Foundational Security Best Practices	EventBridge.3	EventBridge3.
AWS Foundational Security Best Practices	EventBridge.4	EventBridge.4

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	FSx.1	FSx.1
AWS Foundational Security Best Practices	GuardDuty.1	GuardDuty.1
AWS Foundational Security Best Practices	IAM.1	IAM.1
AWS Foundational Security Best Practices	IAM.2	IAM.2
AWS Foundational Security Best Practices	IAM.3	IAM.3
AWS Foundational Security Best Practices	IAM.4	IAM.4
AWS Foundational Security Best Practices	IAM.5	IAM.5
AWS Foundational Security Best Practices	IAM.6	IAM.6
AWS Foundational Security Best Practices	IAM.7	IAM.7
AWS Foundational Security Best Practices	IAM.8	IAM.8

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	IAM.9	IAM.9
AWS Foundational Security Best Practices	IAM.10	IAM.10
AWS Foundational Security Best Practices	IAM.11	IAM.11
AWS Foundational Security Best Practices	IAM.12	IAM.12
AWS Foundational Security Best Practices	IAM.13	IAM.13
AWS Foundational Security Best Practices	IAM.14	IAM.14
AWS Foundational Security Best Practices	IAM.15	IAM.15
AWS Foundational Security Best Practices	IAM.16	IAM.16
AWS Foundational Security Best Practices	IAM.17	IAM.17
AWS Foundational Security Best Practices	IAM.18	IAM.18

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	IAM.19	IAM.19
AWS Foundational Security Best Practices	IAM.21	IAM.21
AWS Foundational Security Best Practices	IAM.22	IAM.22
AWS Foundational Security Best Practices	Kinesis.1	Kinesis.1
AWS Foundational Security Best Practices	KMS.1	KMS.1
AWS Foundational Security Best Practices	KMS.2	KMS.2
AWS Foundational Security Best Practices	KMS.3	KMS.3
AWS Foundational Security Best Practices	KMS.4	KMS.4
AWS Foundational Security Best Practices	Lambda.1	Lambda.1
AWS Foundational Security Best Practices	Lambda.2	Lambda.2

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	Lambda.3	Lambda.3
AWS Foundational Security Best Practices	Lambda.5	Lambda.5
AWS Foundational Security Best Practices	Macie.1	Macie.1
AWS Foundational Security Best Practices	MQ.5	MQ.5
AWS Foundational Security Best Practices	MQ.6	MQ.6
AWS Foundational Security Best Practices	MSK.1	MSK.1
AWS Foundational Security Best Practices	MSK.2	MSK.2
AWS Foundational Security Best Practices	Neptune.1	Neptune.1
AWS Foundational Security Best Practices	Neptune.2	Neptune.2
AWS Foundational Security Best Practices	Neptune.3	Neptune.3

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	Neptune.4	Neptune.4
AWS Foundational Security Best Practices	Neptune.5	Neptune.5
AWS Foundational Security Best Practices	Neptune.6	Neptune.6
AWS Foundational Security Best Practices	Neptune.7	Neptune.7
AWS Foundational Security Best Practices	Neptune.8	Neptune.8
AWS Foundational Security Best Practices	Neptune.9	Neptune.9
AWS Foundational Security Best Practices	NetworkFirewall.1	NetworkFirewall.1
AWS Foundational Security Best Practices	NetworkFirewall.2	NetworkFirewall.2
AWS Foundational Security Best Practices	NetworkFirewall.3	NetworkFirewall.3
AWS Foundational Security Best Practices	NetworkFirewall.4	NetworkFirewall.4

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	NetworkFirewall.5	NetworkFirewall.5
AWS Foundational Security Best Practices	NetworkFirewall.6	NetworkFirewall.6
AWS Foundational Security Best Practices	NetworkFirewall.9	NetworkFirewall.9
AWS Foundational Security Best Practices	Opensearch.1	Opensearch.1
AWS Foundational Security Best Practices	Opensearch.2	Opensearch.2
AWS Foundational Security Best Practices	Opensearch.3	Opensearch.3
AWS Foundational Security Best Practices	Opensearch.4	Opensearch.4
AWS Foundational Security Best Practices	Opensearch.5	Opensearch.5
AWS Foundational Security Best Practices	Opensearch.6	Opensearch.6
AWS Foundational Security Best Practices	Opensearch.7	Opensearch.7

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	Opensearch.8	Opensearch.8
AWS Foundational Security Best Practices	Opensearch.10	Opensearch.10
AWS Foundational Security Best Practices	PCA.1	PCA.1
AWS Foundational Security Best Practices	RDS.1	RDS.1
AWS Foundational Security Best Practices	RDS.2	RDS.2
AWS Foundational Security Best Practices	RDS.3	RDS.3
AWS Foundational Security Best Practices	RDS.4	RDS.4
AWS Foundational Security Best Practices	RDS.5	RDS.5
AWS Foundational Security Best Practices	RDS.6	RDS.6
AWS Foundational Security Best Practices	RDS.7	RDS.7

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	RDS.8	RDS.8
AWS Foundational Security Best Practices	RDS.9	RDS.9
AWS Foundational Security Best Practices	RDS.10	RDS.10
AWS Foundational Security Best Practices	RDS.11	RDS.11
AWS Foundational Security Best Practices	RDS.12	RDS.12
AWS Foundational Security Best Practices	RDS.13	RDS.13
AWS Foundational Security Best Practices	RDS.14	RDS.14
AWS Foundational Security Best Practices	RDS.15	RDS.15
AWS Foundational Security Best Practices	RDS.16	RDS.16
AWS Foundational Security Best Practices	RDS.17	RDS.17

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	RDS.18	RDS.18
AWS Foundational Security Best Practices	RDS.19	RDS.19
AWS Foundational Security Best Practices	RDS.20	RDS.20
AWS Foundational Security Best Practices	RDS.21	RDS.21
AWS Foundational Security Best Practices	RDS.22	RDS.22
AWS Foundational Security Best Practices	RDS.23	RDS.23
AWS Foundational Security Best Practices	RDS.24	RDS.24
AWS Foundational Security Best Practices	RDS.25	RDS.25
AWS Foundational Security Best Practices	RDS.26	RDS.26
AWS Foundational Security Best Practices	RDS.27	RDS.27

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	RDS.34	RDS.34
AWS Foundational Security Best Practices	RDS.35	RDS.35
AWS Foundational Security Best Practices	Redshift.1	Redshift.1
AWS Foundational Security Best Practices	Redshift.2	Redshift.2
AWS Foundational Security Best Practices	Redshift.3	Redshift.3
AWS Foundational Security Best Practices	Redshift.4	Redshift.4
AWS Foundational Security Best Practices	Redshift.6	Redshift.6
AWS Foundational Security Best Practices	Redshift.7	Redshift.7
AWS Foundational Security Best Practices	Redshift.8	Redshift.8
AWS Foundational Security Best Practices	Redshift.9	Redshift.9

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	Redshift.10	Redshift.10
AWS Foundational Security Best Practices	Route53.2	Route53.2
AWS Foundational Security Best Practices	S3.1	S3.1
AWS Foundational Security Best Practices	S3.2	S3.2
AWS Foundational Security Best Practices	S3.3	S3.3
AWS Foundational Security Best Practices	S3.4	S3.4
AWS Foundational Security Best Practices	S3.5	S3.5
AWS Foundational Security Best Practices	S3.6	S3.6
AWS Foundational Security Best Practices	S3.7	S3.7
AWS Foundational Security Best Practices	S3.8	S3.8

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	S3.9	S3.9
AWS Foundational Security Best Practices	S3.11	S3.11
AWS Foundational Security Best Practices	S3.12	S3.12
AWS Foundational Security Best Practices	S3.13	S3.13
AWS Foundational Security Best Practices	S3.14	S3.14
AWS Foundational Security Best Practices	S3.15	S3.15
AWS Foundational Security Best Practices	S3.17	S3.17
AWS Foundational Security Best Practices	S3.19	S3.19
AWS Foundational Security Best Practices	S3.19	S3.20
AWS Foundational Security Best Practices	SageMaker.1	SageMaker.1

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	SageMaker.2	SageMaker.2
AWS Foundational Security Best Practices	SageMaker.3	SageMaker.3
AWS Foundational Security Best Practices	SecretsManager.1	SecretsManager.1
AWS Foundational Security Best Practices	SecretsManager.2	SecretsManager.2
AWS Foundational Security Best Practices	SecretsManager.3	SecretsManager.3
AWS Foundational Security Best Practices	SecretsManager.4	SecretsManager.4
AWS Foundational Security Best Practices	SNS.1	SNS.1
AWS Foundational Security Best Practices	SNS.2	SNS.2
AWS Foundational Security Best Practices	SQS.1	SQS.1
AWS Foundational Security Best Practices	SSM.1	SSM.1

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	SSM.2	SSM.2
AWS Foundational Security Best Practices	SSM.3	SSM.3
AWS Foundational Security Best Practices	SSM.4	SSM.4
AWS Foundational Security Best Practices	StepFunctions.1	StepFunctions.1
AWS Foundational Security Best Practices	WAF.1	WAF.1
AWS Foundational Security Best Practices	WAF.2	WAF.2
AWS Foundational Security Best Practices	WAF.3	WAF.3
AWS Foundational Security Best Practices	WAF.4	WAF.4
AWS Foundational Security Best Practices	WAF.6	WAF.6
AWS Foundational Security Best Practices	WAF.7	WAF.7

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	WAF.8	WAF.8
AWS Foundational Security Best Practices	WAF.10	WAF.10
AWS Foundational Security Best Practices	WAF.11	WAF.11
AWS Foundational Security Best Practices	WAF.12	WAF.12

Additional resources

- To find help with evidence collection issues for this data source type, see My assessment isn't collecting compliance check evidence from AWS Security Hub.
- To create a custom control using this data source type, see Creating a custom control in AWS Audit Manager.
- To create a custom framework that uses your custom control, see Creating a custom framework in AWS Audit Manager.
- To add your custom control to an existing custom framework, see Editing a custom framework in AWS Audit Manager.

AWS API calls supported by AWS Audit Manager

You can use Audit Manager to capture snapshots of your AWS environment as evidence for audits. When you create or edit a custom control, you can specify one or more AWS API calls as a data

source mapping for evidence collection. Audit Manager then makes API calls to the relevant AWS services, and collects a snapshot of the configuration details for your AWS resources.

For every resource that's in the scope of an API call, Audit Manager captures a configuration snapshot and converts it into evidence. This results in one piece of evidence per resource, as opposed to one piece of evidence per API call.

For example, if the `ec2_DescribeRouteTables` API call captures configuration snapshots from five route tables, then you'll get five pieces of evidence in total for the single API call. Each piece of evidence is a snapshot of the configuration of an individual route table.

Topics

Key points

Paginated API calls

Many AWS services collect and store a large amount of data. As a result, when a `list`, `describe`, or `get` API call attempts to return your data, there can be a lot of results. If the amount of data is too large to return in a single response, the results can be broken into more manageable pieces through the use of *pagination*. This divides the results into "pages" of data, making the responses easier to handle.

Some of the Supported API calls for custom control data sources are paginated. This means that they return partial results at first, and require subsequent requests to return the entire result set. For example, the Amazon RDS DescribeDBInstances operation returns up to 100 instances at a time, and subsequent requests are needed to return the next page of results.

As of March 08, 2023, Audit Manager supports paginated API calls as a data source for evidence collection. Previously, if a paginated API call was used as a data source, only a subset of your resources was returned in the API response (up to 100 results). Now, Audit Manager calls the paginated API operation multiple times, and gets each page of results until all resources are returned. For each resource, Audit Manager then captures a configuration snapshot and saves it

as evidence. Because your complete set of resources is now captured in the API response, it's likely that you'll notice an increase in the amount of evidence that's collected after March 08, 2023.

Audit Manager handles API call pagination for you automatically. If you create a custom control that uses a paginated API call as a data source, you don't need to specify any pagination parameters.

Supported API calls for custom control data sources

In your custom controls, you can use any of the following API calls as a data source. Audit Manager can then use these API calls to collect evidence about your AWS usage.

Supported API call	How Audit Manager uses this API to collect evidence
acm_GetAccountConfiguration	Collect a snapshot of the account configuration options associated with your AWS account.
acm_ListCertificates	Retrieve a list of certificate ARNs and domain names.
autoscaling_DescribeAutoScalingGroups	Collect a snapshot about the Auto Scaling groups in your AWS account.
backup_ListBackupPlans	Retrieve a list of all active backup plans in your AWS account.
bedrock_GetModelInvocationLoggingConfiguration	Collect a snapshot of the current configuration values for model invocation logging for models in your AWS account.
cloudfront_ListDistributions	Retrieve a list of all distributions in your AWS account.
cloudtrail_DescribeTrails	Collect a snapshot of the settings for one or more trails associated with the current Region for your AWS account.
cloudtrail_ListTrails	Retrieve a list of the trails that are in your AWS account.

Supported API call	How Audit Manager uses this API to collect evidence
cloudwatch_DescribeAlarms	Collect a configuration snapshot of the alarms that are used for your AWS account.
config_DescribeConfigRules	Retrieve details about your AWS Config rules.
config_DescribeDeliveryChannels	Collect a configuration snapshot for the delivery channels in your in your AWS account.
directconnect_DescribeDirectConnectGateways	Retrieve a list of all your AWS Direct Connect gateways .
directconnect_DescribeVirtualGateways	Retrieve a list of the virtual private gateways owned by your AWS account.
docdb_DescribeCertificates	Collect a list of certificates for your AWS account.
docdb_DescribeDBClusterParameterGroups	Collect a list of `DBClusterParameterGroup` descriptions for your AWS account.
docdb_DescribeDBInstances	Collect information about provisioned Amazon DynamoDB instances for your AWS account.
cloudwatch_DescribeAlarms	Collect information about the alarms in your AWS account.
cloudtrail_DescribeTrails	Collect a snapshot of the settings for one or more trails associated with your AWS account.

Supported API call	How Audit Manager uses this API to collect evidence
dynamodb_DescribeTable	Collect configuration snapshots for the DynamoDB tables in your AWS account. When you use this API as a data source, you don't need to provide the name of a specific DynamoDB table. Instead, Audit Manager uses the `ListTables` operation to list all of your tables. For every table that's listed, Audit Manager then performs the `DescribeTable` operation to generate evidence for that resource.
dynamodb_ListBackups	Retrieve a list of the DynamoDB backups that are associated with your AWS account.
dynamodb_ListTables	Retrieve a list of all of the table names that are associated with your AWS account and your current endpoint.
ec2_DescribeAddresses	Collect a snapshot of your Elastic IP addresses.
ec2_DescribeCustomerGateways	Collect a snapshot of your VPN customer gateways.
ec2_DescribeEgressOnlyInternetGateways	Collect a snapshot of your egress-only internet gateways.
ec2_DescribeFlowLogs	Collect a snapshot of your flow logs.
ec2_DescribeInstances	Collect a snapshot of your instances.
ec2_DescribeInternetGateways	Collect a snapshot of your internet gateways.

Supported API call	How Audit Manager uses this API to collect evidence
ec2_DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations	Collect a description of the associations between the virtual interface groups and the local gateway route tables in your AWS account.
ec2_DescribeLocalGateways	Collect a snapshot of your local gateways.
ec2_DescribeLocalGatewayVirtualInterfaces	Collect a snapshot of your local gateway virtual interfaces.
ec2_DescribeNatGateways	Collect a snapshot of your NAT gateways.
ec2_DescribeNetworkAcls	Collect a snapshot of your network ACLs.
ec2_DescribeRouteTables	Collect a snapshot of your route tables.
ec2_DescribeSecurityGroups	Collect a snapshot of your security groups.
ec2_DescribeSecurityGroupRules	Collect a snapshot of one or more of your security group rules.
ec2_DescribeTransitGateways	Collect a snapshot of your transit gateways.
ec2_DescribeVolumes	Collect a snapshot of your VPC endpoints.
ec2_DescribeVpcs	Collect a snapshot of your VPCs.

Supported API call	How Audit Manager uses this API to collect evidence
ec2_DescribeVpcEndpoints	Collect a snapshot of your VPC endpoints.
ec2_DescribeVpcEndpointConnections	Collect a snapshot of the VPC endpoint connections to your VPC endpoint services, including any endpoints that are pending your acceptance.
ec2_DescribeVpcEndpointServiceConfigurations	Collect a snapshot of the VPC endpoint service configurations in your AWS account.
ec2_DescribeVpcPeeringConnections	Collect a snapshot of your VPN connections.
ec2_DescribeVpnConnections	Collect a snapshot of your VPN connections.
ec2_DescribeVpnGateways	Collect a snapshot of your virtual private gateways.
ec2_GetEbsDefaultKmsKeyId	Collect a snapshot of the default AWS KMS key for EBS encryption for your AWS account in the current Region.
ec2_GetEbsEncryptionByDefault	Describe whether EBS encryption by default is enabled for your AWS account in the current Region.
ecs_DescribeClusters	Collect a snapshot of your ECS clusters.
eks_DescribeAddonVersions	Collect a snapshot of your add-on versions.
elasticache_DescribeCacheClusters	Collect a snapshot of your provisioned clusters.

Supported API call	How Audit Manager uses this API to collect evidence
elasticache_DescribeServiceUpdates	Collect a snapshot of service updates for Amazon ElastiCache.
elasticfilesystem_DescribeAccessPoints	Collect a snapshot of the Amazon EFS access points in your AWS account.
elasticfilesystem_DescribeFileSystems	Collect a snapshot of your Amazon EFS file systems.
elasticloadbalancingv2_DescribeLoadBalancers	Collect a snapshot of the load balancers in your AWS account.
elasticloadbalancingv2_DescribeSSLPolicies	Collect a snapshot of the policies that you use for SSL negotiation.
elasticloadbalancingv2_DescribeTargetGroups	Collect a snapshot of your ELB target groups.
elasticmapreduce_ListSecurityConfigurations	Retrieve a list of the security configurations that are visible to your AWS account, along with their creation dates and times, and their names.
events_ListConnections	Retrieve a list of the Amazon EventBridge connections in your AWS account.
events_ListEventBuses	Retrieve a list of the Amazon EventBridge event buses in your AWS account, including the default event bus, custom event buses, and partner event buses.
events_ListEventSources	Retrieve a list of the partner event sources that have been shared with your AWS account.

Supported API call	How Audit Manager uses this API to collect evidence
events_ListRules	Retrieve a list of your Amazon EventBridge rules.
firehose_ListDeliveryStreams	Retrieve a list of your delivery streams.
fsx_DescribeFileSystems	Collect a snapshot of the file systems that are owned by your AWS account.
guardduty_ListDetectors	Retrieve a list of the `detectorIds` for your Amazon GuardDuty detector resources.
iam_GenerateCredentialReport	Generate a credential report for your AWS account.
iam_GetAccountPasswordPolicy	Collect a snapshot of the password policy for your AWS account.
iam_GetAccountSummary	Collect a snapshot of the IAM entity usage and IAM quotas in your AWS account.
iam_ListGroups	Retrieve a list of the IAM groups that are associated with a path prefix that's available in your AWS account.
iam_ListOpenIDConnectProviders	Retrieve a list of the IAM OpenID Connect (OIDC) provider resource objects that are defined in your AWS account.
iam_ListPolicies	Retrieve a list of all the managed policies that are available in your AWS account, including your own customer-defined managed policies and all AWS managed policies.
iam_ListRoles	Retrieve a list of the IAM roles that are associated with a path prefix that's available in your AWS account.

Supported API call	How Audit Manager uses this API to collect evidence
iam_ListSAMLProviders	Retrieve a list of the SAML provider resource objects defined in IAM in your AWS account.
iam_ListUsers	Retrieve a list of the IAM users in your AWS account.
iam_ListVirtualMFADevices	Retrieve a list of the virtual MFA devices that are defined in your AWS account.
kafka_ListClusters	Retrieve a list of the Amazon MSK clusters in your AWS account.
kafka_ListKafkaVersions	Retrieve a list of the Apache Kafka version objects in your AWS account.
kinesis_ListStreams	Retrieve a list of your Kinesis data streams.
kms_GetKeyPolicy	Audit Manager uses this API to collect a snapshot of the key policies for the AWS KMS keys in your AWS account. When you use this API as a data source, you don't need to provide the name of a specific AWS KMS key. Instead, Audit Manager uses the `ListKeys` operation to list all of your KMS keys. For every KMS key that's listed, Audit Manager then performs the `GetKeyPolicy` operation to generate evidence for that resource.
kms_GetKeyRotationStatus	Audit Manager uses this API to collect a snapshot of whether automatic rotation is enabled for the AWS KMS keys in your AWS account. When you use this API as a data source, you don't need to provide the name of a specific AWS KMS key. Instead, Audit Manager uses the `ListKeys` operation to list all of your KMS keys. For every KMS key that's listed, Audit Manager then performs the `GetKeyRotationStatus` operation to generate evidence for that resource.
kms_ListKeys	Retrieve a list of the AWS KMS keys in your AWS account.
lambda_ListFunctions	Retrieve a list of Lambda functions in your AWS account, with the version-specific configuration of each.

Supported API call	How Audit Manager uses this API to collect evidence
rds_DescribeDBClusters	Collect a snapshot of the existing Amazon Aurora DB clusters and Multi-AZ DB clusters in your AWS account.
rds_DescribeDBInstances	Collect a snapshot of the provisioned RDS instances in your AWS account.
rds_DescribeDbInstanceAutomatedBackups	Collect a snapshot of the backups for both current and deleted instances in your AWS account.
rds_DescribeDbSecurityGroups	Collect a snapshot of the DBSecurityGroups in your AWS account.
redshift_DescribeClusters	Collect a snapshot of the provisioned Amazon Redshift clusters in your AWS account.
s3_GetBucketEncryption	Collect a snapshot that shows the default encryption configuration for your S3 buckets. When you use this API as a data source, you don't need to provide the name of a specific S3 bucket. Instead, Audit Manager uses the `ListBuckets` operation to list the buckets that were created in the same AWS Region as your assessment. For every bucket that's listed, Audit Manager then performs the `GetBucketEncryption` operation to generate evidence for that resource. Audit Manager can only provide the encryption status for buckets that were created in the same AWS Region as your assessment. If you need to see the encryption status of all your S3 buckets across multiple AWS Regions, we recommend that you create an assessment in each AWS Region where you have an S3 bucket.

Supported API call	How Audit Manager uses this API to collect evidence
s3_ListBuckets	Retrieve a list of the S3 buckets in your AWS account. Audit Manager can only list buckets that were created in the same AWS Region as your assessment. If you need to see all your S3 buckets across multiple AWS Regions, we recommend that you create an assessment in each AWS Region where you have an S3 bucket.
sagemaker_ListAlgorithms	Retrieve a list of the machine learning algorithms in your AWS account.
sagemaker_ListDomains	Retrieve a list of the domains in your AWS account.
sagemaker_ListEndpoints	Retrieve a list of the endpoints in your AWS account.
sagemaker_ListEndpointConfigs	Retrieve a list of the endpoint configurations in your AWS account.
sagemaker_ListFlowDefinitions	Retrieve a list of the flow definitions in your AWS account.
sagemaker_ListHumanTaskUis	Retrieve a list of the human task interfaces in your AWS account.
sagemaker_ListLabelingJobs	Retrieve a list of the labeling jobs in your AWS account.
sagemaker_ListModels	Retrieve a list of the models in your AWS account.
sagemaker_ListModelBiasJobDefinitions	Retrieve a list of the model bias job definitions in your AWS account.

Supported API call	How Audit Manager uses this API to collect evidence
sagemaker_ListModelCards	Retrieve a list of the model cards in your AWS account.
sagemaker_ListModelQualityJobDefinitions	Retrieve a list of the model quality monitoring job definitions in your AWS account.
sagemaker_ListMonitoringAlerts	Retrieve a list of the alerts for a given monitoring schedule.
sagemaker_ListMonitoringSchedules	Retrieve a list of all monitoring schedules in your AWS account.
sagemaker_ListTrainingJobs	Retrieve a list of training jobs in your AWS account.
sagemaker_ListUserProfiles	Retrieve a list of user profiles in your AWS account.
secretsmanager_ListSecrets	Retrieve a list of the secrets that are stored in your AWS account, not including secrets that are marked for deletion.
sns_ListTopics	Retrieve a list of the SNS topics in your AWS account.
sqs_ListQueues	Retrieve a list of the SQS queues in your AWS account.
waf-regional_ListWebAcls	Retrieve a list of the WebACLSummary objects for your AWS account.
waf-regional_ListRules	Retrieve a list of the RuleSummary objects for your AWS account.
waf_ListRuleGroups	Retrieve a list of the RuleGroupSummary objects for the rule groups in your AWS account.
waf_ListRules	Retrieve a list of the RuleSummary objects for your AWS account.

Supported API call	How Audit Manager uses this API to collect evidence
waf_ListWebAcls	Retrieve a list of the WebACLSummary objects for your AWS account.

API calls used in the AWS License Manager standard framework

In the AWS License Manager standard framework, Audit Manager uses a custom activity called `GetLicenseManagerSummary` to collect evidence. This activity calls the following three License Manager APIs:

- ListLicenseConfigurations
- ListAssociationsForLicenseConfiguration
- ListUsageForLicenseConfiguration

The data that's returned is then converted into evidence and attached to the relevant controls in your assessment.

Example

Let's say that you use two licensed products (*SQL Service 2017* and *Oracle Database Enterprise Edition*). First, the `GetLicenseManagerSummary` activity calls the ListLicenseConfigurations API, which provides details of license configurations in your account. Next, it adds additional contextual data for each license configuration by calling ListUsageForLicenseConfiguration and ListAssociationsForLicenseConfiguration. Finally, it converts the license configuration data into evidence and attaches it to the respective controls in the framework (*4.5 - Customer managed license for SQL Server 2017* and *3.0.4 - Customer managed license for Oracle Database Enterprise Edition*).

If you're using a licensed product that isn't covered by any of the controls in the framework, that license configuration data is attached as evidence to the following control: *5.0 - Customer managed license for other licenses*.

Additional resources

- To find help with evidence collection issues for this data source type, see My assessment isn't collecting configuration data evidence for an AWS API call.

- To create a custom control using this data source type, see Creating a custom control in AWS Audit Manager.
- To create a custom framework that uses your custom control, see Creating a custom framework in AWS Audit Manager.
- To add your custom control to an existing custom framework, see Editing a custom framework in AWS Audit Manager.

AWS CloudTrail event names supported by AWS Audit Manager

You can use Audit Manager to capture AWS CloudTrail management events and global service events as evidence for audits. When you create or edit a custom control, you can specify one or more CloudTrail event names as a data source mapping for evidence collection. Audit Manager then filters your CloudTrail logs based on your chosen keywords, and imports the results as user activity evidence.

> **Note**
>
> Audit Manager captures management events and global service events only. Data events and insights events are not available as evidence. For more information about the different types of CloudTrail events, see CloudTrail concepts in the *AWS CloudTrail User Guide*.

As an exception to the above, the following CloudTrail events aren't supported by Audit Manager:

- kms_GenerateDataKey
- kms_Decrypt
- sts_AssumeRole
- kinesisvideo_GetDataEndpoint
- kinesisvideo_GetSignalingChannelEndpoint
- kinesisvideo_DescribeSignalingChannel
- kinesisvideo_DescribeStream

As of May 11, 2023, Audit Manager no longer supports read-only CloudTrail events as keywords for evidence collection. We removed a total of 3,135 read-only keywords. Because customers and AWS

services both make read calls to APIs, read-only events are noisy. As a result, read-only keywords collect a lot of evidence that isn't reliable or relevant for audits. Read-only keywords include `List`, `Describe`, and `Get` API calls (for example, GetObject and ListBuckets for Amazon S3). If you were using one of these keywords for evidence collection, you don't need to do anything. The keywords were automatically removed from the Audit Manager console and from your assessments, and evidence is no longer collected for these keywords.

Additional resources

- To find help with evidence collection issues for this data source type, see My assessment isn't collecting user activity evidence from AWS CloudTrail.
- To create a custom control using this data source type, see Creating a custom control in AWS Audit Manager.
- To create a custom framework that uses your custom control, see Creating a custom framework in AWS Audit Manager.
- To add your custom control to an existing custom framework, see Editing a custom framework in AWS Audit Manager.

Setting up AWS Audit Manager with the recommended settings

Before you start using Audit Manager, it's important that you complete the following setup tasks.

This chapter will walk you through the prerequisites, account setup, user permissions, and the necessary steps to enable and configure Audit Manager with the recommended features and integrations. After completing these tasks, you'll be ready to use Audit Manager and get started with streamlining your audit and compliance efforts.

Contents

Prerequisites for setting up AWS Audit Manager

Before you can use AWS Audit Manager, you must make sure that you have properly set up your AWS account and user permissions.

This page outlines the necessary steps to create an AWS account (if needed), configure an administrative user, and grant the permissions required to access and enable Audit Manager.

Tasks

1. Sign up for an AWS account
2. Create a user with administrative access
3. Add the required permissions to access and enable Audit Manager

> **Important**
>
> If you're already set up with AWS and IAM, you can skip tasks 1 and 2. However, you must complete task 3 to ensure that you have the required permissions to set up Audit Manager.

Sign up for an AWS account

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 or text message and entering a verification code on the phone keypad.

   When you sign up for an AWS account, an *AWS account root user* is created. The root user has access to all AWS services and resources in the account. As a security best practice, assign administrative access to a user, and use only the root user to perform tasks that require root user access.

AWS sends you a confirmation email after the sign-up process is complete. At any time, you can view your current account activity and manage your account by going to https://aws.amazon.com/ and choosing **My Account**.

Create a user with administrative access

After you sign up for an AWS account, secure your AWS account root user, enable AWS IAM Identity Center, and create an administrative user so that you don't use the root user for everyday tasks.

Secure your AWS account root user

1. Sign in to the AWS Management Console as the account owner by choosing **Root user** and entering your AWS account email address. On the next page, enter your password.

   For help signing in by using root user, see Signing in as the root user in the *AWS Sign-In User Guide*.

2. Turn on multi-factor authentication (MFA) for your root user.

   For instructions, see Enable a virtual MFA device for your AWS account root user (console) in the *IAM User Guide*.

Create a user with administrative access

1. Enable IAM Identity Center.

   For instructions, see Enabling AWS IAM Identity Center in the *AWS IAM Identity Center User Guide*.

2. In IAM Identity Center, grant administrative access to a user.

   For a tutorial about using the IAM Identity Center directory as your identity source, see Configure user access with the default IAM Identity Center directory in the *AWS IAM Identity Center User Guide*.

Sign in as the user with administrative access

- To sign in with your IAM Identity Center user, use the sign-in URL that was sent to your email address when you created the IAM Identity Center user.

  For help signing in using an IAM Identity Center user, see Signing in to the AWS access portal in the *AWS Sign-In User Guide*.

Assign access to additional users

1. In IAM Identity Center, create a permission set that follows the best practice of applying least-privilege permissions.

   For instructions, see Create a permission set in the *AWS IAM Identity Center User Guide*.
2. Assign users to a group, and then assign single sign-on access to the group.

   For instructions, see Add groups in the *AWS IAM Identity Center User Guide*.

Add the required permissions to access and enable Audit Manager

You must give users the required permissions to enable Audit Manager. For users who need full access to Audit Manager, use the AWSAuditManagerAdministratorAccess managed policy. This is an AWS managed policy that's available in your AWS account, and it's the recommended policy for Audit Manager administrators.

> **Tip**
>
> As a security best practice, we recommend that you get started with AWS managed policies and then move toward least-privilege permissions. AWS managed policies grant permissions for many common use cases. However, keep in mind that because AWS managed policies are available for use by all AWS customers, they might not grant least-privilege permissions for your specific use cases. As a result, we recommend that you reduce permissions further by defining customer managed policies that are specific to your use cases. For more information, see AWS managed policies in the *AWS Identity and Access Management User Guide.*

To provide access, add permissions to your users, groups, or roles:

- Users and groups in AWS IAM Identity Center:

  Create a permission set. Follow the instructions in Create a permission set in the *AWS IAM Identity Center User Guide*.
- Users managed in IAM through an identity provider:

Create a role for identity federation. Follow the instructions in Create a role for a third-party identity provider (federation) in the *IAM User Guide*.

- IAM users:
  - Create a role that your user can assume. Follow the instructions in Create a role for an IAM user in the *IAM User Guide*.
  - (Not recommended) Attach a policy directly to a user or add a user to a user group. Follow the instructions in Adding permissions to a user (console) in the *IAM User Guide*.

Next steps

Now that you've set up your AWS account and granted the required permissions, you're ready to enable Audit Manager. For step-by-step instructions, see Enabling AWS Audit Manager.

Enabling AWS Audit Manager

Now that you have completed the prerequisites for setting up Audit Manager, you can enable the service in your AWS environment.

On this page you'll learn how to enable Audit Manager using the Audit Manager console, the AWS Command Line Interface (AWS CLI), or the Audit Manager API. Choose the method that best suits your needs, and follow the corresponding steps to get Audit Manager up and running.

Prerequisites

Make sure that you completed all of the tasks that are described in Prerequisites for setting up AWS Audit Manager.

Procedure

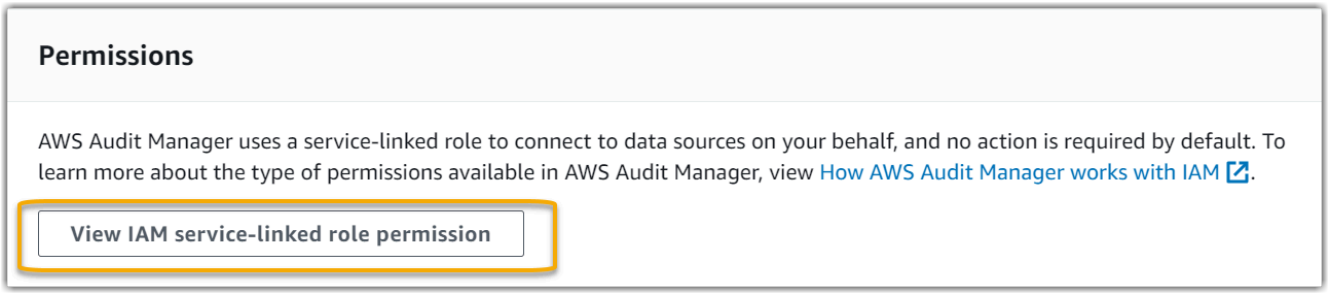
You can enable Audit Manager using the AWS Management Console, the Audit Manager API, or the AWS Command Line Interface (AWS CLI).

Audit Manager console

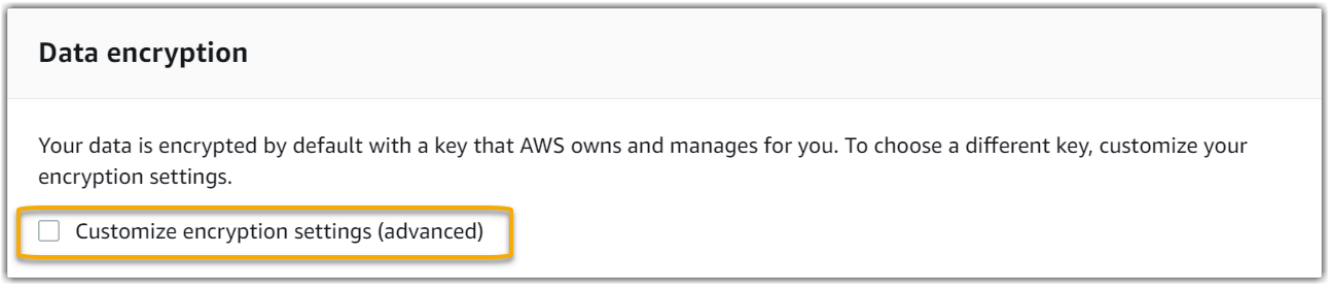
To enable Audit Manager using the console

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. Use the credentials of your IAM identity to sign in.
3. Choose **Set up AWS Audit Manager**.

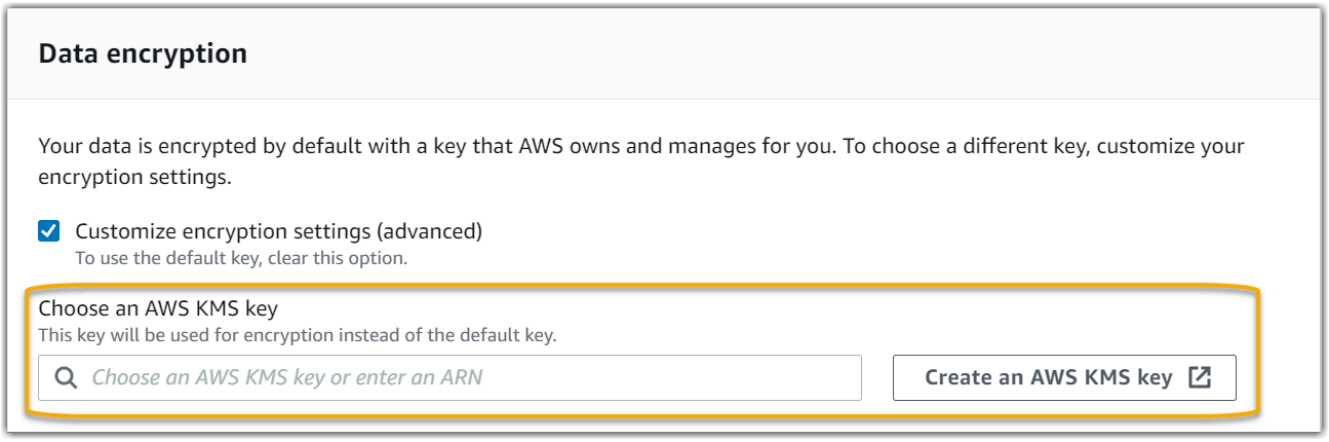
4. Under **Permissions**, no action is required. This is because Audit Manager uses a service-linked role to connect to data sources on your behalf. You can review the service-linked role by choosing **View IAM service-linked role permission**.



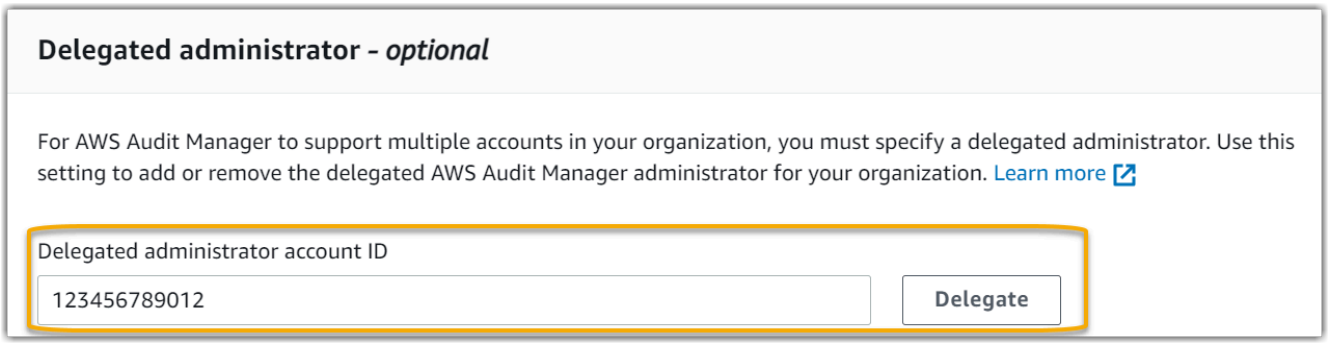
5. Under **Data encryption**, the default option is for Audit Manager to create and manage an AWS KMS key for securely storing your data.



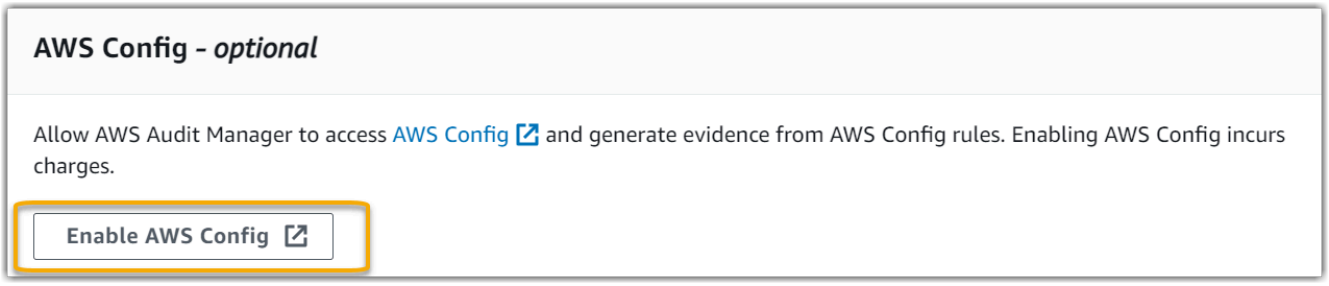
If you want to use your own customer managed key to encrypt data in Audit Manager, select the check box next to **Customize encryption settings (advanced)**. You can then choose an existing KMS key or create a new one.



6. (Optional) Under **Delegated administrator - optional**, you can specify a delegated administrator account if you want Audit Manager to run assessments for multiple accounts. For more information and recommendations, see Enable and set up AWS Organizations.

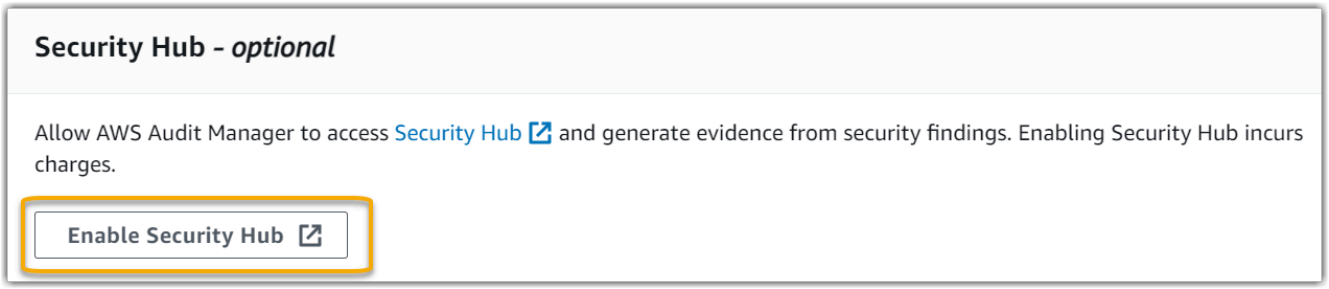


7. (Optional) Under **AWS Config – optional**, we recommend that you enable AWS Config for an optimal experience. This enables Audit Manager to generate evidence using AWS Config rules. For instructions and recommended settings, see Enable and set up AWS Config.



8. (Optional) Under **Security Hub – optional**, we recommend that you enable Security Hub for an optimal experience. This enables Audit Manager to generate evidence using Security

Hub checks. For instructions and recommended settings, see Enable and set up AWS Security Hub.



9. Choose **Complete setup** to finish the setup process.

AWS CLI

To enable Audit Manager using the AWS CLI

In the command line, run the register-account command using the following setup parameters:

- `--kms-key` (optional) – Use this parameter to encrypt your Audit Manager data using your own customer managed key. If you don't specify an option here, Audit Manager creates and manages an AWS KMS key on your behalf for the secure storage of your data.
- `--delegated-admin-account` (optional) – Use this parameter to designate your organization's delegated administrator account for Audit Manager. If you don't specify an option here, no delegated administrator is registered.

Input example (replace the *placeholder text* with your own information):

```
aws auditmanager register-account \
--kms-key arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab \
--delegated-admin-account 111122224444
```

Output example:

```
{
```

```
    "status": "ACTIVE"
}
```

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

Audit Manager API

To enable Audit Manager using the Audit Manager API

Use the RegisterAccount operation with the following setup parameters:

- kmsKey (optional) – Use this parameter to encrypt your Audit Manager data using your own customer managed key. If you don't specify an option here, Audit Manager creates and manages an AWS KMS key on your behalf for the secure storage of your data.
- delegatedAdminAccount (optional) – Use this parameter to specify your organization's delegated administrator account for Audit Manager. If you don't specify one, no delegated administrator is registered.

Input example (replace the *placeholder text* with your own information):

```
{
    "kmsKey":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "delegatedAdminAccount":"111122224444"
}
```

Output example:

```
{
  "status": "ACTIVE"
}
```

Next steps

After you enable Audit Manager, we recommend that you set up some recommended features and integrations for an optimal experience. For more information, see Enabling the recommended features and AWS services for AWS Audit Manager.

Enabling the recommended features and AWS services for AWS Audit Manager

Now that you have enabled AWS Audit Manager, it's time to set up the recommended features and integrations to get the most out of the service.

Key points

For an optimal experience in Audit Manager, we recommend that you set up the following features and enable the following AWS services.

Tasks

- Set up recommended Audit Manager features
- Set up recommended integrations with other AWS services
  - Enable and set up AWS Config
  - Enable and set up AWS Security Hub
  - Enable and set up AWS Organizations

Set up recommended Audit Manager features

After you enable Audit Manager, we recommend that you enable the evidence finder feature.

Evidence finder provides a powerful way to search for evidence in Audit Manager. Instead of browsing deeply nested evidence folders to find what you're looking for, you can use evidence finder to quickly query your evidence. If you use evidence finder as a delegated administrator, you can search for evidence across all member accounts in your organization.

Using a combination of filters and groupings, you can progressively narrow the scope of your search query. For example, if you want a high-level view of your system health, perform a broad

search and filter by assessment, date range, and resource compliance. If your goal is to remediate a specific resource, you can perform a narrow search to target evidence for a specific control or resource ID. After you define your filters, you can group and then preview the matching search results before creating an assessment report.

Set up recommended integrations with other AWS services

For an optimal experience in Audit Manager, we strongly recommend that you enable the following AWS services:

- **AWS Organizations** – You can use Organizations to run Audit Manager assessments over multiple accounts and consolidate evidence into a delegated administrator account.
- **AWS Security Hub** and **AWS Config** – Audit Manager relies on these AWS services as data sources for evidence collection. When you enable AWS Config and Security Hub, Audit Manager can operate with its full functionality, collecting comprehensive evidence and accurately reporting the results of compliance checks directly from these services.

> **Important**
>
> If you don't enable and configure AWS Config and Security Hub, you won't be able to collect the intended evidence for many controls in your Audit Manager assessments. As a result, you risk incomplete or failed evidence collection for certain controls. More specifically:
>
> - If Audit Manager attempts to use AWS Config as a control data source, but the required AWS Config rules aren't enabled, no evidence will be collected for those controls.
> - Similarly, if Audit Manager attempts to use Security Hub as a control data source, but the required standards aren't enabled in Security Hub, no evidence will be collected for those controls.
>
> To mitigate these risks and ensure comprehensive evidence collection, follow the steps on this page to enable and configure AWS Config and Security Hub before you create your Audit Manager assessments.

Enable and set up AWS Config

Many controls in Audit Manager require AWS Config as a data source type. To support these controls, you must enable AWS Config on all accounts in each AWS Region where Audit Manager is enabled.

Audit Manager doesn't manage AWS Config for you. You can follow these steps to enable AWS Config and configure its settings.

> **Important**
>
> Enabling AWS Config is an optional recommendation. However, if you do enable AWS Config, the following settings are required. If Audit Manager tries to collect evidence for controls that use AWS Config as a data source type, and AWS Config is not set up as described below, no evidence is collected for those controls.

Tasks to integrate AWS Config with Audit Manager

- Step 1: Enable AWS Config
- Step 2: Configure your AWS Config settings for use with Audit Manager

Step 1: Enable AWS Config

You can enable AWS Config using the AWS Config console or API. For instructions, see Getting started with AWS Config in the *AWS Config Developer Guide*.

Step 2: Configure your AWS Config settings for use with Audit Manager

After you enable AWS Config, make sure that you also enable AWS Config rules or deploy a conformance pack for the compliance standard that's related to your audit. This step ensures that Audit Manager can import findings for the AWS Config rules that you enabled.

After you enable an AWS Config rule, we recommend that you review the parameters of that rule. You should then validate those parameters against the requirements of your chosen compliance framework. If needed, you can update a rule's parameters in AWS Config to ensure that it aligns with framework requirements. This will help to ensure that your assessments collect the correct compliance check evidence for a given framework.

For example, suppose that you're creating an assessment for CIS v1.2.0. This framework has a control named 1.4 – Ensure access keys are rotated every 90 days or less. In AWS Config, the

access-keys-rotated rule has a `maxAccessKeyAge` parameter with a default value of 90 days. As a result, the rule aligns with the control requirements. If you aren't using the default value, ensure that the value you're using is equal to or greater than the 90 day requirement from CIS v1.2.0.

You can find the default parameter details for each managed rule in the AWS Config documentation. For instructions on how to configure a rule, see Working with AWS Config Managed Rules.

Enable and set up AWS Security Hub

Many controls in Audit Manager require Security Hub as a data source type. To support these controls, you must enable Security Hub on all accounts in each Region where Audit Manager is enabled.

Audit Manager doesn't manage Security Hub for you. You can follow these steps to enable Security Hub and configure its settings.

> **Important**
>
> Enabling Security Hub is an optional recommendation. However, if you do enable Security Hub, the following settings are required. If Audit Manager tries to collect evidence for controls that use Security Hub as a data source type, and Security Hub is not set up as described below, no evidence is collected for those controls.

Tasks to integrate AWS Security Hub with Audit Manager

- Step 1: Enable AWS Security Hub
- Step 2: Configure your Security Hub settings for use with Audit Manager
- Step 3: Configure the Organizations settings for your organization

Step 1: Enable AWS Security Hub

You can enable Security Hub using either the console or the API. For instructions, see Setting up AWS Security Hub in the *AWS Security Hub User Guide*.

Step 2: Configure your Security Hub settings for use with Audit Manager

After you enable Security Hub, make sure that you also do the following:

- Enable AWS Config and configure resource recording – Security Hub uses service-linked AWS Config rules to perform most of its security checks for controls. To support these controls, AWS Config must be enabled and configured to record resources that are required for the controls that you have enabled in each enabled standard.
- Enable all security standards – This step ensures that Audit Manager can import findings for all supported compliance standards.
- Turn on the consolidated control findings setting in Security Hub - This setting is turned *on* by default if you enable Security Hub on or after February 23, 2023.

> **Note**
>
> When you enable consolidated findings, Security Hub produces a single finding for each security check (even when the same check is used across multiple standards). Each Security Hub finding is collected as one unique resource assessment in Audit Manager. As a result, consolidated findings results in a decrease of the total unique resource assessments that Audit Manager performs for Security Hub findings. For this reason, using consolidated findings can often result in a reduction in your Audit Manager usages costs. For more information about using Security Hub as a data source type, see AWS Security Hub controls supported by AWS Audit Manager. For more information about Audit Manager pricing, see AWS Audit Manager Pricing.

Step 3: Configure the Organizations settings for your organization

If you use AWS Organizations and you want to collect Security Hub evidence from your member accounts, you must also perform the following steps in Security Hub.

To set up your organization's Security Hub settings

1. Sign in to the AWS Management Console and open the AWS Security Hub console at https://console.aws.amazon.com/securityhub/.
2. Using your AWS Organizations management account, designate an account as the delegated administrator for Security Hub. For more information, see Designating a Security Hub administrator account in the *AWS Security Hub User Guide*.

> **Note**
>
> Make sure that the delegated administrator account that you designate in Security Hub is the same one that you use in Audit Manager.

3. Using your Organizations delegated administrator account, go to **Settings, Accounts**, select all accounts, and then add them as members by selecting **Auto-enroll**. For more information, see Enabling member accounts from your organization in the *AWS Security Hub User Guide*.
4. Enable AWS Config for every member account of the organization. For more information, see Enabling member accounts from your organization in the *AWS Security Hub User Guide*.
5. Enable the PCI DSS security standard for every member account of the organization. The AWS CIS Foundations Benchmark standard and the AWS Foundational Best Practices standard are already enabled by default. For more information, see Enabling a security standard in the *AWS Security Hub User Guide*.

Enable and set up AWS Organizations

Audit Manager supports multiple accounts via integration with AWS Organizations. Audit Manager can run assessments over multiple accounts and consolidate evidence into a delegated administrator account. The delegated administrator has permissions to create and manage Audit Manager resources with the organization as the zone of trust. Only the management account can designate a delegated administrator.

> **Important**
>
> Enabling AWS Organizations is an optional recommendation. However, if you do enable AWS Organizations, the following settings are required.

Tasks to integrate AWS Organizations with Audit Manager

- Step 1: Create or join an organization
- Step 2: Enable all features in your organization
- Step 3: Specify a delegated administrator for Audit Manager

Step 1: Create or join an organization

If your AWS account isn't part of an organization, you can create or join an organization. For instructions, see Creating and managing an organization in the *AWS Organizations User Guide*.

Step 2: Enable all features in your organization

Next, you must enable all features in your organization. For instructions, see Enabling all features in your organization in the *AWS Organizations User Guide*.

Step 3: Specify a delegated administrator for Audit Manager

We recommend that you enable Audit Manager using an Organizations management account, and then specify a delegated administrator. After that, you can use the delegated administrator account to log in and run assessments. As a best practice, we recommend that you only create assessments using the delegated administrator account instead of the management account.

To add or change a delegated administrator after you enable Audit Manager, see Adding a delegated administrator and Changing a delegated administrator.

Next steps

Now that you have set up Audit Manager with the recommended settings, you're ready to get started with using the service.

- To get started with your first assessment, see Tutorial for Audit Owners: Creating an assessment.
- To update your settings in the future, see Reviewing and configuring your AWS Audit Manager settings.

Getting started with AWS Audit Manager

Use the step-by-step tutorials in this section to learn how to perform tasks using AWS Audit Manager.

Tip

The following tutorials are categorized by audience. Choose the tutorial that's appropriate for you based on your role as an *audit owner* or *delegate*.

- **Audit owners** are Audit Manager users who are responsible for creating and managing assessments. In the business world, audit owners are typically governance, risk management, and compliance (GRC) professionals. In the context of Audit Manager, however, individuals from SecOps or DevOps teams might also assume the user persona of an audit owner. Audit owners can request assistance from a subject matter expert—also known as a delegate—to review specific controls and validate evidence. Audit owners must have the necessary permissions to manage an assessment.
- **Delegates** are subject matter experts with specialized technical or business expertise. Although they don't own or manage Audit Manager assessments, they can still contribute to them. Delegates assist audit owners with tasks such as validating evidence for the controls that fall under their area of expertise. Delegates have limited permissions in Audit Manager. This is because audit owners delegate specific control sets for review, and not entire assessments.

For more information about these personas and other Audit Manager concepts, see audit owner and delegate in the Understanding AWS Audit Manager concepts and terminology section of this guide.
For more information about the recommended IAM permissions for each persona, see Recommended policies for user personas in AWS Audit Manager.

Audit Manager tutorials

Creating an assessment

Audience: Audit owners

Overview: Follow step-by-step instructions to create your first assessment and get up and running fast. This tutorial walks you through how you can use a standard framework to create an assessment and begin the automated collection of evidence.

Reviewing a control set

Audience: Delegates

Overview: Assist an audit owner by reviewing evidence for controls that fall under your area of expertise. Learn to review control sets and their related evidence, add comments, upload evidence, and update the status of a control.

Tutorial for Audit Owners: Creating an assessment

This tutorial provides an introduction to AWS Audit Manager. In this tutorial, you create an assessment using the AWS Audit Manager Sample Framework. By creating an assessment, you start the ongoing process of automated evidence collection for the controls in that framework.

> **Note**
>
> AWS Audit Manager assists in collecting evidence that's relevant for verifying compliance with specific compliance frameworks and regulations. However, it doesn't assess your compliance itself. The evidence that's collected through AWS Audit Manager therefore might not include all the information about your AWS usage that's needed for audits. AWS Audit Manager isn't a substitute for legal counsel or compliance experts.

Prerequisites

Before you start this tutorial, make sure that you meet the following conditions:

- You completed all the prerequisites that are described in Setting up AWS Audit Manager with the recommended settings. You must use your AWS account and the AWS Audit Manager console to complete this tutorial.
- Your IAM identity is granted with the appropriate permissions to create and manage an assessment in AWS Audit Manager. Two suggested policies that grant these permissions are Allow users full administrator access to AWS Audit Manager and Allow users management access to AWS Audit Manager.

- You're familiar with Audit Manager terminology and functionality. For a general overview, see What is AWS Audit Manager? and Understanding AWS Audit Manager concepts and terminology.

Procedure

Tasks

- Step 1: Specify assessment details
- Step 2: Specify AWS accounts in scope
- Step 3: Specify audit owners
- Step 4: Review and create

Step 1: Specify assessment details

For the first step, select a framework and provide basic information for your assessment.

To specify assessment details

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. Choose **Launch AWS Audit Manager**.
3. In the green banner at the top of the screen, choose **Start with a framework**.
4. Choose the framework that you want, and then choose **Create assessment from framework**. For this tutorial, use the **AWS Audit Manager Sample Framework**.
5. Under **Assessment name**, enter a name for your assessment.
6. (Optional) Under **Assessment description**, enter a description for your assessment.
7. Under **Assessment reports destination**, choose the S3 bucket where you want to save your assessment reports.
8. Under **Frameworks**, confirm that **AWS Audit Manager Sample Framework** is selected.
9. (Optional) Under **Tags**, choose **Add new tag** to associate a tag with your assessment. You can specify a key and a value for each tag. The tag key is mandatory and can be used as a search criteria when you search for this assessment.
10. Choose **Next**.

Step 2: Specify AWS accounts in scope

Next, specify the AWS accounts that you want to include in the scope of your assessment.

AWS Audit Manager integrates with AWS Organizations, so you can run an Audit Manager assessment across multiple accounts and consolidate evidence into a delegated administrator account. To enable Organizations in Audit Manager (if you didn't do so already), see Enable and set up AWS Organizations on the *Setting up* page of this guide.

> **Note**
>
> Audit Manager can support up to 200 accounts in the scope of an assessment. If you try to include over 200 accounts, the assessment creation will fail.
> Additionally, if you try to add over 250 unique accounts across all of your assessments, the assessment creation will fail.

To specify accounts in scope

1. Under **AWS accounts**, select the AWS accounts that you want to include in the scope of your assessment.
   - If you enabled Organizations in Audit Manager, multiple accounts are listed.
   - If you didn't enable Organizations in Audit Manager, only your current account is listed.
2. Choose **Next**.

Step 3: Specify audit owners

In this step, you specify the audit owners for your assessment. Audit owners are the individuals in your workplace—usually from GRC, SecOps, or DevOps teams—who are responsible for managing the Audit Manager assessment. We recommend that they use the AWSAuditManagerAdministratorAccess policy.

To specify audit owners

1. Under **Audit owners**, choose the audit owners for your assessment. To find additional audit owners, use the search bar to search by name or AWS account.
2. Choose **Next**.

Step 4: Review and create

Review the information for your assessment. To change the information for a step, choose **Edit**. When you're finished, choose **Create assessment** to start the ongoing collection of evidence.

After you create an assessment, evidence collection continues until you change the assessment status to *inactive*. Alternatively, you can stop evidence collection for a specific control by changing the control status to *inactive*.

> **Note**
>
> Automated evidence is available 24 hours after you create the assessment. Audit Manager automatically collects evidence from multiple data sources, and the frequency of that evidence collection is based on the evidence type. For more information, see Evidence collection frequency in this guide.

Additional resources

We recommend that you continue to learn more about the concepts and tools that are introduced in this tutorial. You can do so by reviewing the following resources:

- **Reviewing assessment details in AWS Audit Manager –** Introduces you to the assessment details page where you can explore the different components of your assessment.
- **Managing assessments in AWS Audit Manager –** Builds upon this tutorial and provides in-depth information about the concepts and tasks for managing an assessment. In this chapter, we particularly recommend you check out the following topics:
  - How to create an assessment from a different framework
  - How to review the evidence in an assessment and generate an assessment report
  - How to change the status of an assessment or delete an assessment
- **Using the framework library to manage frameworks in AWS Audit Manager –** Introduces the framework library and explains how to create a custom framework for your own specific compliance needs.
- **Using the control library to manage controls in AWS Audit Manager –** Introduces the control library and explains how to create a custom control for use in your custom framework.

- **Understanding AWS Audit Manager concepts and terminology –** Provides definitions for the concepts and terminology used in Audit Manager.
- [Video] Collect Evidence and Manage Audit Data Using AWS Audit Manager– Shows the assessment creation process that's described in this tutorial, and other tasks such as reviewing a control and generating an assessment report.

Tutorial for Delegates: Reviewing a control set

This tutorial describes how to review a control set that was shared with you by an audit owner in AWS Audit Manager.

Audit owners use Audit Manager to create assessments and collect evidence for the controls in that assessment. Sometimes audit owners might have questions or need assistance when validating the evidence for a control set. In this situation, an audit owner can delegate a control set to a subject matter expert for review.

As a delegate, you help audit owners to review the collected evidence for controls that fall under your area of expertise.

Prerequisites

Before you start this tutorial, make sure that you first meet the following conditions:

- Your AWS account is set up. To complete this tutorial, you must use both your AWS account and the Audit Manager console. For more information, see Setting up AWS Audit Manager with the recommended settings.
- You're familiar with Audit Manager terminology and functionality. For a general overview of Audit Manager, see What is AWS Audit Manager? and Understanding AWS Audit Manager concepts and terminology.

Procedure

Tasks

- Step 1: Review your notifications
- Step 2: Review the control set and related evidence
- Step 3. Add manual evidence (optional)

- Step 4. Add a comment for a control (optional)
- Step 5: Mark a control as reviewed (optional)
- Step 6. Submit the reviewed control set back to the audit owner

Step 1: Review your notifications

Start by signing in to Audit Manager where you can access your notifications to see the control sets that have been delegated to you for review.

To review your notifications

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the left navigation pane, choose **Notifications**.
3. On the **Notifications** page, you review the list of control sets that have been delegated to you. The notifications table includes the following information:

Name	Description
Date	The date when the control set was delegated.
Assessment	The name of the assessment that's associated with the control set. You can choose an assessment name to open the assessment detail page.
Control set	The name of the control set that was delegated to you for review.
Source	The user or role that delegated the control set to you.
Description	The review instructions that were provided by the audit owner.

Tip

You can also subscribe to an SNS topic to receive email alerts when a control set is assigned to you for review. For more information, see Notifications in AWS Audit Manager.

Step 2: Review the control set and related evidence

The next step is to review the control sets that the audit owner delegated to you. By examining the controls and their evidence, you can determine if any additional action is needed for a control. Additional actions can include manually uploading additional evidence to demonstrate compliance, or leaving a comment about that control.

To review a control set

1. From the **Notifications** page, review the list of control sets that were delegated to you. Then identify which one you want to review and choose the name of the related assessment.
2. Under the **Controls** tab of the assessment detail page, scroll down to the **Control sets** table.
3. Under the **Controls grouped by control set** column, expand the name of a control set to show its controls. Then, choose the name of a control to open the control detail page.
4. (Optional) Choose **Update control status** to change the status of the control. While your review is in progress, you can mark the status as **Under review**.
5. Review information about the control in the **Evidence folders**, **Details**, **Evidence sources**, **Comments**, and **Changelog** tabs. To learn about each of these tabs and how to understand the data that they contain, see Reviewing an assessment control in AWS Audit Manager.

To review the evidence for a control

1. From the control detail page, choose the **Evidence folders** tab.
2. Navigate to the **Evidence folders** table, where a list of folders that contains evidence for that control is displayed. These folders are organized and named based on the date when the evidence within that folder was collected.
3. Choose the name of an evidence folder to open it. From here, you can review a summary of all the evidence that was gathered on that date. To understand this information, see Reviewing an evidence folder in AWS Audit Manager.
4. From the evidence folder summary page, navigate to the **Evidence** table. Under the **Time** column, choose a line item to open and review details of the evidence that was collected at that time. To understand this information, see Reviewing evidence in AWS Audit Manager.

Step 3. Add manual evidence (optional)

Although AWS Audit Manager automatically collects evidence for many controls, in some cases you might need to provide additional evidence. In these cases, you can manually add your own evidence that helps you to demonstrate compliance with that control.

To add manual evidence to a control

There are several ways to add manual evidence to a control. You can import a file from Amazon S3, upload a file from your browser, or enter a text response. For instructions for each method, see Adding manual evidence in AWS Audit Manager.

Step 4. Add a comment for a control (optional)

You can add comments for any controls that you review. These comments are visible to the audit owner. For example, you can leave a comment to provide a status update and confirm that you remediated any issues with that control.

To add a comment to a control

1. From the **Notifications** page, review the list of control sets that were delegated to you. Find the control set that you want to leave a comment for, and choose the name of the related assessment.
2. Choose the **Controls** tab, scroll down to the **Control sets** table, and then select the name of a control to open it.
3. Choose the **Comments** tab.
4. Under **Send comments**, enter your comment in the text box.
5. Choose **Submit comments** to add your comment. Your comment now appears under the **Previous comments** section of the page, along with any other comments regarding this control.

Step 5: Mark a control as reviewed (optional)

Changing the status of a control is optional. However, we recommend that you change the status of each control to **Reviewed** as you complete your review for that control. Regardless of the status of each individual control, you can still submit the controls to the audit owner.

To mark a control as reviewed

1. From the **Notifications** page, review the list of control sets that were delegated to you. Find the control set that contains the control that you want to mark as reviewed. Then, choose the name of the related assessment to open the assessment detail page.
2. Under the **Controls** tab of the assessment detail page, scroll down to the **Control sets** table.
3. Under the **Controls grouped by control set** column, expand the name of a control set to show its controls. Choose the name of a control to open the control detail page.
4. Choose **Update control status** and change the status to **Reviewed**.
5. In the pop-up window that appears, choose **Update control status** to confirm that you finished reviewing the control.

Step 6. Submit the reviewed control set back to the audit owner

When you're done reviewing all controls, submit the control set back to the audit owner to let them know you finished your review.

To submit a reviewed control set back to the owner

1. In the **Notifications** page, review the list of control sets that were assigned to you. Find the control set that you want to submit to the audit owner, and choose the name of the related assessment.
2. Scroll down to the **Control sets** table, select the control set that you want to submit back to the audit owner, and then choose **Submit for review**.
3. In the pop-up window that appears, you can add any high-level comments about that control set before choosing **Submit for review**.

After you submit the control to the audit owner, the audit owner can view any comments that you left for them.

Additional resources

You can continue to learn more about the concepts that are introduced in this tutorial. Here are some recommended resources:

- Reviewing assessment details in AWS Audit Manager - Introduces you to the assessment details page, where you can explore the different components of an Audit Manager assessment.

- Reviewing an assessment control in AWS Audit Manager and Reviewing evidence in AWS Audit Manager - Provides definitions to help you understand the controls and evidence in an assessment.
- Understanding AWS Audit Manager concepts and terminology - Provides definitions for the concepts and terminology that are used in Audit Manager.

Using the Audit Manager dashboard

With the Audit Manager dashboard, you can visualize non-compliant evidence in your active assessments. It's a convenient and fast way to monitor your assessments, stay informed, and remediate issues proactively. By default, the dashboard provides a top-down, aggregated view of all your active assessments. Using this view, you can visually identify issues in your assessments without first needing to sift through vast amounts of individual evidence.

The dashboard is the first screen that you see when you sign in to the Audit Manager console. It contains two widgets that show the data and key performance indicators (KPIs) that are most relevant to you. Using an assessment filter, you can refine this data to focus on the KPIs for a specific assessment. From there, you can review control domain groupings to identify which controls have the most non-compliant evidence. Then, you can explore the underlying controls to examine and remediate issues.

> **Note**
>
> If you're a first-time Audit Manager user or you don't have any active assessments, no data is displayed in the dashboard. To get started, create an assessment. This starts the ongoing collection of evidence. After a 24-hour period, aggregated evidence data will start to appear in the dashboard. You can read the following sections to learn how to understand and interpret this data.

This page covers the following topics:

Topics

Dashboard concepts and terminology

This section covers important things to know about the Audit Manager dashboard before you get started using it.

Permissions and visibility

Both audit owners and delegates have access to the dashboard. This means that both of these personas can see the metrics and aggregates for all active assessments in your AWS account. Having access to the same information enables all of your team to focus on the same KPIs and goals.

Filters

Audit Manager provides a page-level the section called “Assessment filter” that you can apply to all of the widgets on your dashboard.

Non-compliant evidence

The dashboard highlights the controls in your assessments that have compliance check evidence with a *non-compliant* conclusion. Compliance check evidence relates to controls that use AWS Config or AWS Security Hub as a data source type. For this evidence type, Audit Manager reports the result of a compliance check directly from those services. If Security Hub reports a *Fail* result, or if AWS Config reports a *Non-compliant* result, Audit Manager classes the evidence as non-compliant.

Inconclusive evidence

Evidence is *inconclusive* if a compliance check isn’t available or applicable. As a result, no compliance evaluation can be made. This is the case if a control uses AWS Config or AWS Security Hub as a data source type but you didn’t enable those services. This is also the case if the control uses a data source type that doesn't support compliance checks, such as manual evidence, AWS API calls, or AWS CloudTrail. In the console, evidence with a compliance check status of *not applicable* is classified as *inconclusive* in the dashboard.

You can use the inconclusive evidence to manually evaluate a control's compliance.

> **Note**
>
> Inconclusive evidence doesn't indicate failure, it signals that you should manually evaluate the evidence for compliance.

Compliant evidence

Evidence is *compliant* if a compliance check reported no issues. This is the case if Security Hub reports a *Pass* result, or AWS Config reports a *Compliant* result.

Control domains

The dashboard introduces the concept of a *control domain*. You can think of a control domain as a general category of controls that isn't specific to any one framework. Control domain groupings are one of the most powerful features of the dashboard. Audit Manager highlights the controls in your assessments that have non-compliant evidence, and groups them by control domain. Using this feature, you can focus your remediation efforts on specific subject domains as you prepare for an audit.

> **Note**
>
> A control domain is different to a *control set*. A control set is a framework-specific grouping of controls that's typically defined by a regulatory body. For example, the PCI DSS framework has a control set named *Requirement 8: Identify and authenticate access to system components*. This control set falls under the control domain of *Identity and access management*.

Eventual consistency of data

The dashboard data is *eventually consistent*. This means that, when you read data from the dashboard, it might not instantly reflect the results of a recently completed write or update operation. If you check again within a few hours, the dashboard should reflect the latest data.

Data from deleted and inactive assessments

The dashboard displays data from active assessments. If you delete an assessment or change its status to inactive on the same day that you view the dashboard, data is included for that assessment as follows.

- **Inactive assessments** – If Audit Manager collected evidence for your assessment before you changed it to inactive, that evidence data is included in the dashboard counts for that day.
- **Deleted assessments** – If Audit Manager collected evidence for your assessment before you deleted it, that evidence data isn't included in the dashboard counts for that day.

Dashboard elements

The following sections cover the different components of the dashboard.

Topics

Assessment filter

You can use the assessment filter to focus on a specific active assessment.

By default, the dashboard displays aggregated data for all your active assessments. If you want to view data for a specific assessment, you apply an assessment filter. This is a page-level filter that applies to all widgets on the dashboard.

To apply the assessment filter, select an assessment from the drop-down list at the top of the dashboard. This list shows up to 10 of your active assessments. The most recently created assessments appear first. If you have many active assessments, you can start typing the name of an assessment to quickly find it. After you select an assessment, the dashboard displays data for that assessment only.

Daily snapshot

This widget shows a snapshot of the current compliance status of your active assessments.

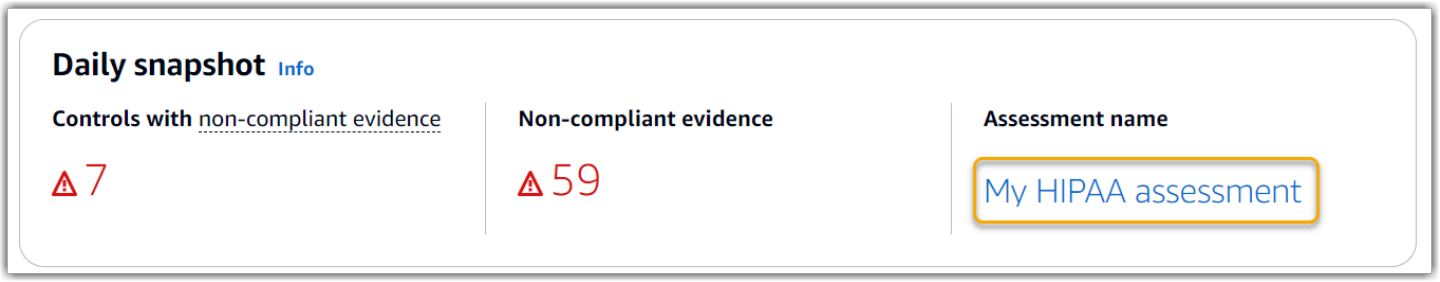
The daily snapshot reflects the latest data that was collected on the date at the top of the dashboard. The date and time on the dashboard are represented in Coordinated Universal Time (UTC). It's important to understand that these numbers are daily counts based on this timestamp. They aren't a total sum to date.

By default, the daily snapshot shows the following data for all your active assessments:

1. **Controls with non-compliant evidence** - The total number of controls that are associated with non-compliant evidence.
2. **Non-compliant evidence** - The total amount of compliance check evidence with a non-compliant conclusion.

3. **Active assessments** - The total number of your active assessments. Choose this number to see links to these assessments.

The daily snapshot data changes based on the the section called "Assessment filter" that you apply. When you specify an assessment, the data reflects the daily counts for that assessment only. In this case, the daily snapshot shows the name of the assessment that you specified. You can choose the name of the assessment to open it.

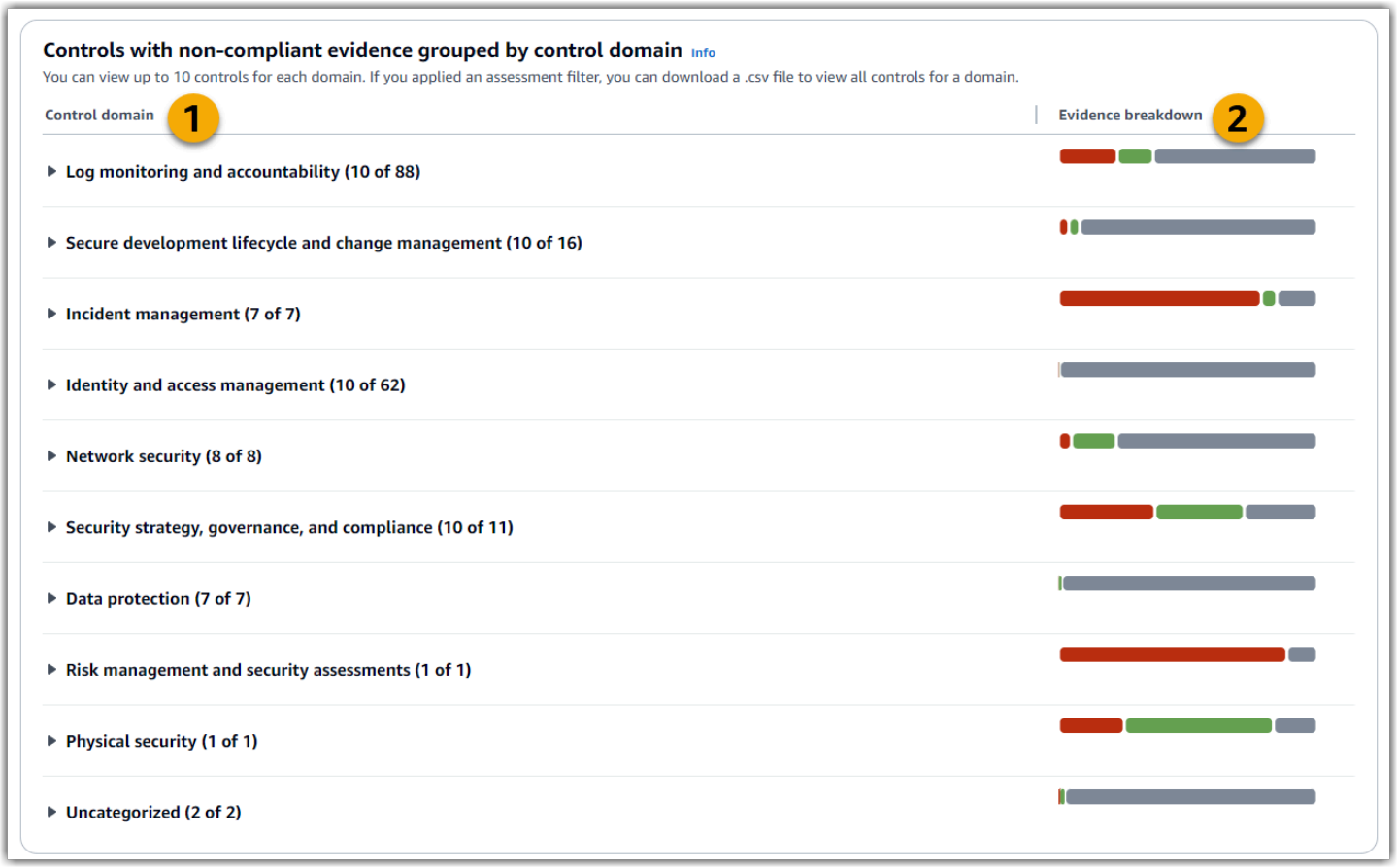


Controls with non-compliant evidence grouped by control domain

You can use this widget to identify which controls have the most non-compliant evidence.

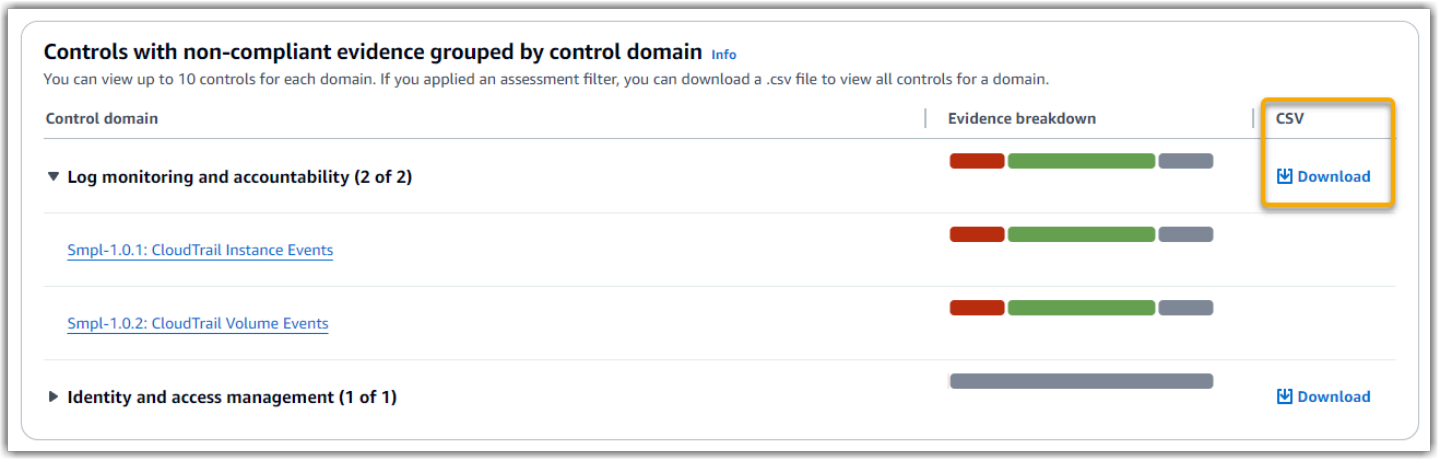
By default, the widget shows the following data for all your active assessments:

1. **Control domain** – A list of the control domains that are associated with your active assessments.
2. **Evidence breakdown** – A bar chart that shows a breakdown of the evidence compliance status.



To expand a control domain, choose the arrow next to its name. When expanded, the console shows up to 10 controls for each domain. These controls are ranked according to the highest total count of non-compliant evidence.

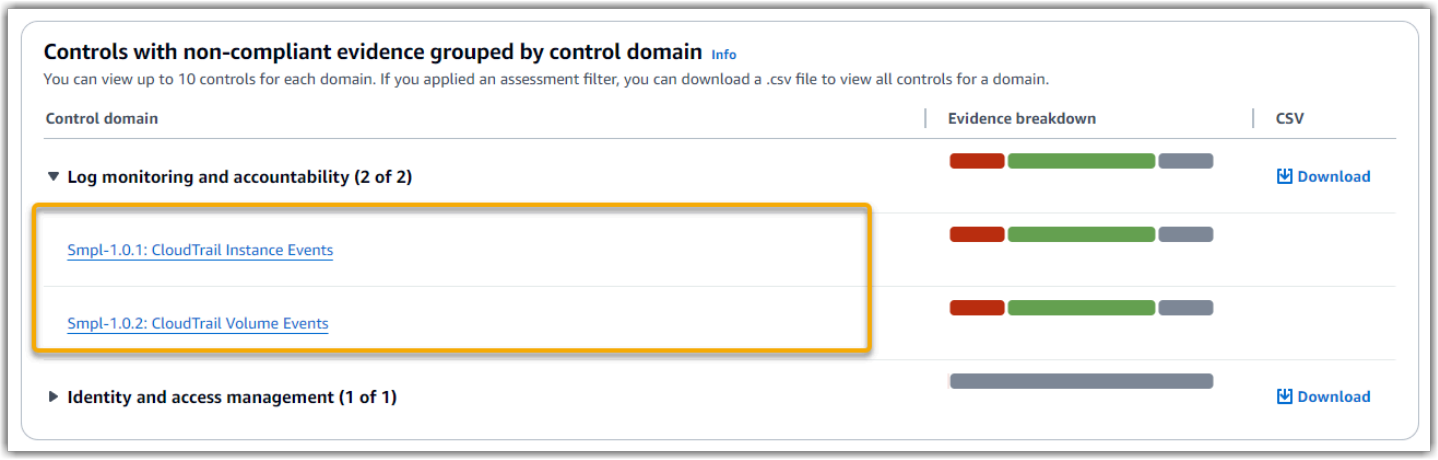
The data in this widget changes based on the the section called "Assessment filter" that you apply. When you specify an assessment, you see data for that assessment only. In addition, you can also download a CSV file for each available control domain in the assessment.



The .csv file includes the full list of controls in the domain that are associated with non-compliant evidence. The following example shows the CSV data columns with fictionalized values.

	A	B	C	D	E	F	G
1	Date and Time	AssessmentID	AsessmentName	ControlId	ControlName	ControlDescription	DataSource
2	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	abcdefgh-1234-bcde-5678-cdefghijklmn	Control 1	Description of control 1	Manual
3	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	12345678-abcd-9012-bcde-345678901234	Control 2	Description of control 2	Manual
4	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	bcdefghi-2345-cdef-3456-defghijklmno	Control 3	Description of control 3	AWS Config, AWS Security Hub
5	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	23456789-bcde-0123-cdef-456789012345	Control 4	Description of control 4	Manual
6	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	cdefghij-3456-defg-4567-efghijklmnop	Control 5	Description of control 5	AWS Config
7	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	34567890-cdef-1234-defg-567890123456	Control 6	Description of control 6	Manual
8	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	defghijk-4567-efgh-5678-fghijklmnopq	Control 7	Description of control 7	AWS Config
9	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	45678901-defg-2345-efgh-678901234567	Control 8	Description of control 8	AWS Security Hub
10	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	efghijkl-5678-fghi-6789-ghijklmnopqr	Control 9	Description of control 9	Manual
11	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	56789012-efgh-3456-fghi-789012345678	Control 10	Description of control 10	Manual
12	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	fghijklm-6789-ghij-7890-hijklmnopqrs	Control 11	Description of control 11	Manual
13	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	67890123-fghi-4567-ghij-890123456789	Control 12	Description of control 12	Manual
14	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	ghijklmn-7890-hijk-8901-ijklmnopqrst	Control 13	Description of control 13	AWS Config, AWS Security Hub
15	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	78901234-ghij-5678-hijk-901234567890	Control 14	Description of control 14	Manual
16							

Lastly, when you apply an assessment filter, the control names under each domain are hyperlinked. Choose any control to open the control details page in the specified assessment.



Tip

Using the control details page as your starting point, you can move from one level of detail to the next.

1. **Control details page** - On this page, the Evidence folders tab lists daily folders of evidence that Audit Manager collected for that control. For more detail, choose a folder.
2. **Evidence folder -** Next, you can review an Evidence folder summary and a list of the evidence in that folder. For more detail, choose an individual evidence item.
3. **Individual evidence** - Lastly, you can explore individual evidence details. This is the most granular level of evidence data.

Next steps

Here are some next steps that you can take after reviewing the dashboard.

- **Download a CSV file** – Find the assessment and control domain that you want to focus on, and download the full list of related controls with non-compliant evidence.
- **Review a control** – After you identify a control that needs remediation, you can review the control.
- **Delegate a control for review** – If you need assistance reviewing a control, you can delegate a control set for review.
- **Edit your assessment** – If you want to change the scope of an active assessment, you can edit the assessment.
- **Update the status of your assessment** – If you want to stop collecting evidence for an assessment, you can change the assessment status to inactive.

Additional resources

To find answers to common questions and issues, see Troubleshooting dashboard issues in the *Troubleshooting* section of this guide.

Managing assessments in AWS Audit Manager

An Audit Manager assessment is based on a framework, which is a grouping of controls. Using a framework as a starting point, you can create an assessment that collects evidence for the controls in that framework. In your assessment, you can also define the scope of your audit. This includes specifying the AWS accounts that you want to collect evidence for.

Key points

You can create an assessment from any framework. Either, you can use a standard framework that's provided by Audit Manager. Or, you can create an assessment from a custom framework that you build yourself. Standard frameworks contain prebuilt control sets that support a specific compliance standard or regulation. In contrast, custom frameworks contain controls that you can customize and group according to your own requirements.

When you create an assessment, this starts the ongoing collection of evidence. When it's time for an audit, you or a delegate can review this evidence and then add it to an assessment report.

> **Note**
>
> AWS Audit Manager assists in collecting evidence that's relevant for verifying compliance with specific compliance standards and regulations. However, it doesn't assess your compliance itself. The evidence that's collected through AWS Audit Manager therefore might not include all the information about your AWS usage that's needed for audits. AWS Audit Manager isn't a substitute for legal counsel or compliance experts.

Additional resources

To create and manage assessments in Audit Manager, follow the procedures that are outlined here.

- Creating an assessment in AWS Audit Manager
- Finding your assessments in AWS Audit Manager
- Reviewing an assessment in AWS Audit Manager
  - Reviewing assessment details in AWS Audit Manager

Creating an assessment in AWS Audit Manager

This topic builds on the Tutorial for Audit Owners: Creating an assessment. You'll find detailed instructions on this page that show you how to create an assessment from a framework. Follow these steps to create an assessment and start the ongoing collection of evidence.

Prerequisites

Before you start this tutorial, make sure that you meet the following conditions:

- You completed all the prerequisites that are described in Setting up AWS Audit Manager with the recommended settings. You must use your AWS account and the Audit Manager console to complete this tutorial.
- Your IAM identity has appropriate permissions to create and manage an assessment in Audit Manager. Two suggested policies that grant these permissions are AWSAuditManagerAdministratorAccess and Allow users management access to AWS Audit Manager.

Procedure

Tasks

- Step 1: Specify assessment details
- Step 2: Specify AWS accounts in scope
- Step 3: Specify audit owners
  - Audit owner permissions
- Step 4: Review and create

Step 1: Specify assessment details

Start by selecting a framework and providing basic information for your assessment.

To specify assessment details

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the navigation pane, choose **Assessments**, and then choose **Create assessment**.
3. Under **Name**, enter a name for your assessment.
4. (Optional) Under **Description**, enter a description for your assessment.
5. Under **Assessment reports destination**, select the S3 bucket where you want to save your assessment reports.

> **Tip**
>
> The default assessment report destination is based on your assessment settings. If you prefer, you can create and use multiple S3 buckets to help you organize your

assessment reports for different assessments. AWS Audit Manager supports exporting assessment reports to Amazon S3 buckets, including cross-account destinations. For optimal security and performance, we recommend using an S3 bucket in the same AWS account and region as your assessment.

6. Under **Select framework**, select the framework that you want to create your assessment from. You can also use the search bar to look up a framework by name, or by compliance standard or regulation.

> **Tip**
>
> To learn more about a framework, choose the framework name to see the framework details page.

7. (Optional) Under **Tags**, choose **Add new tag** to associate a tag with your assessment. You can specify a key and a value for each tag. The tag key is mandatory and can be used as a search criteria when you search for this assessment.
8. Choose **Next**.

> **Note**
>
> It's important to make sure that your assessment collects the correct evidence for a given framework. Before you start evidence collection, we recommend that you review the requirements for your chosen framework. Then, validate these requirements against your current AWS Config rule parameters. To ensure that your rule parameters align with framework requirements, you can update the rule in AWS Config.
> For example, suppose that you're creating an assessment for CIS v1.2.0. This framework has a control named 1.9 – Ensure IAM password policy requires a minimum length of 14 or greater. In AWS Config, the iam-password-policy rule has a `MinimumPasswordLength` parameter that checks password length. The default value for this parameter is 14 characters. As a result, the rule aligns with the control requirements. If you aren't using the default parameter value, ensure that the value you're using is equal to or greater than the 14 character requirement from CIS v1.2.0. You can find the default parameter details for each managed rule in the AWS Config documentation.

Step 2: Specify AWS accounts in scope

You can specify multiple AWS accounts to be in the scope of an assessment. Audit Manager supports multiple accounts through integration with AWS Organizations. This means that Audit Manager assessments can be run over multiple accounts, and the evidence that's collected is consolidated into a delegated administrator account. To enable Organizations in Audit Manager, see Enable and set up AWS Organizations.

> **Note**
>
> Audit Manager can support up to 200 accounts in the scope of an assessment. If you try to include over 200 accounts, the assessment creation will fail.
> Additionally, if you try to add over 250 unique accounts across all of your assessments, the assessment creation will fail.

To specify AWS accounts in scope

1. Under **AWS accounts**, select the AWS accounts that you want to include in the scope of your assessment.
   - If you enabled Organizations in Audit Manager, multiple accounts are displayed. You can choose one or more accounts from the list. Alternatively, you can also search for an account by the account name, ID, or email.
   - If you didn't enable Organizations in Audit Manager, only your current AWS account is listed.
2. Choose **Next**.

> **Note**
>
> When an in-scope account is removed from your organization, Audit Manager no longer collects evidence for that account. However, the account continues to show in your assessment under the **AWS accounts** tab. To remove the account from the list of accounts in scope, edit the assessment. The removed account no longer shows in the list during editing, and you can save your changes without that account in scope.

Step 3: Specify audit owners

In this step, you specify the audit owners for your assessment. Audit owners are the individuals in your workplace—usually from GRC, SecOps, or DevOps teams—who are responsible for managing the Audit Manager assessment. We recommend that they use the AWSAuditManagerAdministratorAccess policy.

To specify audit owners

1. Under **Audit owners**, review the current list of audit owners. The **Audit owner** column displays the user IDs and roles. The **AWS account** column displays the AWS account of that audit owner.
2. Audit owners that have a selected check box are included in your assessment. Clear the check box for any audit owner to remove them from the assessment. You can find additional audit owners by using the search bar to search by name or AWS account.
3. When you're finished, choose **Next**.

Audit owner permissions

The below policy is attached for all the audit owners of an assessment.

Audit Manager replaces the *placeholder text* with your account and resource identifiers before attaching the policy.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditOwner",
            "Effect": "Allow",
            "Principal": {
                "AWS": "Principal for user/role who are the audit owners of the
 Assessment"
            },
            "Action": [
                "auditmanager:GetAssessment",
                "auditmanager:UpdateAssessment",
                "auditmanager:UpdateAssessmentControlSetStatus",
```

```
                "auditmanager:UpdateAssessmentStatus",
                "auditmanager:UpdateAssessmentControl",
                "auditmanager:DeleteAssessment",
                "auditmanager:GetChangeLogs",
                "auditmanager:GetEvidenceFoldersByAssessment",
                "auditmanager:GetEvidenceFoldersByAssessmentControl",
                "auditmanager:BatchImportEvidenceToAssessmentControl",
                "auditmanager:GetEvidenceFolder",
                "auditmanager:GetEvidence",
                "auditmanager:GetEvidenceByEvidenceFolder",
                "auditmanager:BatchCreateDelegationByAssessment",
                "auditmanager:BatchDeleteDelegationByAssessment",
                "auditmanager:AssociateAssessmentReportEvidenceFolder",
                "auditmanager:BatchAssociateAssessmentReportEvidence",
                "auditmanager:BatchDisassociateAssessmentReportEvidence",
                "auditmanager:CreateAssessmentReport",
                "auditmanager:DeleteAssessmentReport",
                "auditmanager:DisassociateAssessmentReportEvidenceFolder",
                "auditmanager:GetAssessmentReportUrl"
            ],
            "Resource": [
                "arn:aws:auditmanager:us-
east-1:123456789012:assessment/assessment_ID",
                "arn:aws:auditmanager:us-
east-1:123456789012:assessment/assessment_ID/*"
            ]
        }
    ]
}
```

Step 4: Review and create

Review the information for your assessment. To change the information for a step, choose **Edit**. When you're finished, choose **Create assessment**.

This action starts the ongoing collection of evidence for your assessment. After you create an assessment, evidence collection continues until you change the assessment status to *inactive*. Alternatively, you can stop evidence collection for a specific control by change the control status to *inactive*.

> **Note**
>
> Automated evidence becomes available 24 hours after your assessment is created. Audit Manager automatically collects evidence from multiple data sources, and the frequency of that evidence collection is based on the evidence type. To learn more, see Evidence collection frequency in this guide.

Next steps

To revisit your assessment at a later date, see Finding your assessments in AWS Audit Manager. You can follow these steps to locate your assessment so that you can view, edit, or continue working on it.

Additional resources

For solutions to assessment issues in Audit Manager, see Troubleshooting assessment and evidence collection issues.

Finding your assessments in AWS Audit Manager

After you create assessments in AWS Audit Manager, you can find them on the assessments page of the Audit Manager console.

From this page, you can perform various actions on your assessments. For example, you can view assessment details, edit assessment configurations, or delete assessments that are no longer required. Additionally, the assessments page serves as a starting point for creating new assessments.

You can also view your assessments programmatically using the Audit Manager API or the AWS Command Line Interface (AWS CLI).

Prerequisites

The following procedure assumes that you have previously created at least one assessment. If you haven't created an assessment yet, you won't see any results when you follow these steps.

Make sure your IAM identity has appropriate permissions to view an assessment in AWS Audit Manager. Two suggested policies that grant these permissions are

AWSAuditManagerAdministratorAccess and Allow users management access to AWS Audit Manager.

Procedure

You can view your assessments using the Audit Manager console, the Audit Manager API, or the AWS Command Line Interface (AWS CLI).

Audit Manager console

To view your assessments on the Audit Manager console

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the left navigation pane, choose **Assessments** to see a list of your assessments.
3. Choose any assessment name to view the details for that assessment.

AWS CLI

To view your assessments (CLI)

To view assessments in Audit Manager, run the list-assessments command. You can use the `--status` subcommand to view assessments that are active or inactive.

```
aws auditmanager list-assessments --status ACTIVE
```

```
aws auditmanager list-assessments --status INACTIVE
```

Audit Manager API

To view your assessments using the API

To view assessments in Audit Manager, use the ListAssessments operation. You can use the status attribute to view assessments that are active or inactive.

For more information, choose either of the previous links to read more in the *AWS Audit Manager API Reference*. This includes information about how to use the `ListAssessments` operation and parameters in one of the language-specific AWS SDKs.

Next steps

When you're ready to explore your assessment's contents, follow the steps in Reviewing an assessment in AWS Audit Manager. This page will guide you through the assessment details and explain the information that you see there.

From the assessments page, you can also edit an assessment, delete an assessment, or create an assessment.

Additional resources

For solutions to assessment issues in Audit Manager, see Troubleshooting assessment and evidence collection issues.

Reviewing an assessment in AWS Audit Manager

After you create assessments in Audit Manager, you can open and review your assessments at any time.

Key points

When you're ready to explore your assessment, you can gradually dive deeper into the details and review your assessment with increasing levels of granularity.

1. **Assessment details** – Start by reviewing the overall details of your assessment. On this page you can review the assessment name, description, scope, and other details. This gives you a high-level overview of the assessment.
2. **Assessment control details** – Next, dive deeper into the assessment by reviewing the details of each assessment control. This will enable you to understand the specific requirements and objectives of each control.
3. **Evidence folder details** – For each assessment control, you can review the corresponding evidence folders that contain the evidence for a given control. These folders organize the supporting evidence that’s related to each control.
4. **Evidence details** – Lastly, drill down further to review the individual pieces of evidence within each folder. This might include configuration snapshots, user activity logs, compliance findings, or manually uploaded evidence such as documents and screenshots. Reviewing this evidence will help you understand how your organization is meeting the requirements of the control.

By following these steps, you can thoroughly explore your assessment, understand its components, and review the evidence that supports your organization's compliance efforts.

Additional resources

To get started with reviewing an assessment in Audit Manager, follow the procedures that are outlined here.

- Reviewing assessment details in AWS Audit Manager
- Reviewing an assessment control in AWS Audit Manager
- Reviewing an evidence folder in AWS Audit Manager
- Reviewing evidence in AWS Audit Manager

Reviewing assessment details in AWS Audit Manager

When you need to review the details of an assessment, you'll find the information organized into several sections on the assessment details page. These sections help you easily access and understand the relevant information for your task.

Contents

Prerequisites

The following procedure assumes that you have previously created at least one assessment. If you haven't created an assessment yet, you won't see any results when you follow these steps.

Make sure your IAM identity has appropriate permissions to view an assessment in AWS Audit Manager. Two suggested policies that grant these permissions are AWSAuditManagerAdministratorAccess and Allow users management access to AWS Audit Manager.

Procedure

To open and review an assessment details page

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the left navigation pane, choose **Assessments** to see a list of your assessments.
3. Choose the name of the assessment to open it.
4. Review the assessment details using the following information as reference.

Sections of the assessment details page

- Assessment details section
- Controls tab
- Assessment report selection tab
- AWS accounts tab
- AWS services tab
- Audit owners tab
- Tags tab
- Changelog tab

Assessment details section

You can use the **Assessment details** section to see a summary of your assessment.

In the assessment details section, you can review the following information:

Name	Description
1. Description	The description of the assessment.
2. Compliance type	The compliance standard or regulation that the assessment supports.
3. Assessment reports destination	The S3 bucket that Audit Manager saves the assessment report in.
4. Total evidence	The total number of evidence items that are collected for this assessment.
5. Assessment report selection	The number of evidence items that are selected to be included in the assessment report.
6. Date created	The date when the assessment was created.
7. Last updated	The date when the assessment was last edited.
8. Status	The status of the assessment. • **Active** - The assessment is currently collecting evidence. • **Inactive** - The assessment is no longer collecting evidence.

Controls tab

You can use this tab to see information about the controls in the assessment.

Under **Control status summary**, you can review the following information:

Name	Description
Total controls	The total number of controls in this assessment.
Reviewed	The number of controls that were reviewed by an audit owner or a delegate.
Under review	The number of controls that are currently under review.
Inactive	The number of controls that are no longer actively collecting evidence

In the **Control sets** table, you can review a list of controls grouped by control set. You can expand or collapse the controls in each control set. You can also search by name if you're looking for a specific control.

In this table, you can review the following information:

Name	Description
Controls grouped by control sets	The name of the control set.
Control status	The status of the control. • **Under review** indicates that this control isn't already reviewed. Evidence is still being collected for this control, and you can add manual evidence. This is the default status. • **Reviewed** indicates that the evidence for this control was reviewed. Evidence is still being collected, and you can add manual evidence. • **Inactive** indicates that automated evidence collection is stopped for this control. You can no longer add manual evidence.

Name	Description
Delegated to	The reviewer of this control, if it was assigned to a delegate for review.
Total evidence	The number of evidence items that have been collected for this control.

Assessment report selection tab

You can use this tab to see the evidence that will be included in the assessment report. The evidence is grouped by evidence folders, which are organized based on the date when they were created.

You can browse these folders and select which evidence you want to include in your assessment report. For instructions on how to add evidence to an assessment report, see Adding evidence to an assessment report.

In this section, you can review the following information:

Name	Description
Evidence folder	The name of the evidence folder. The folder name is based on the date when the evidence was collected.
Selected evidence	The number of evidence items within the folder that are included in the assessment report.
Control name	The name of the control that's associated with this evidence folder.

AWS accounts tab

You can use this tab to see the AWS accounts that are in the scope of the assessment.

In this section, you can review the following information:

Name	Description
Account ID	The ID of the AWS account.
Account name	The name of the AWS account.
Email	The email address that's associated with the AWS account.

AWS services tab

You might or might not see this tab in your assessment.

If the AWS services tab isn't displayed (ideal state)

If you don't see this tab, Audit Manager is managing which AWS services are in scope for your assessment.

Audit Manager infers this scope by examining your assessment controls and their data sources, and then mapping this information to the corresponding AWS services. Whenever an underlying data source changes for your assessment, Audit Manager automatically updates the scope as needed to reflect the correct AWS services. This ensures that your assessment collects accurate and comprehensive evidence about all of the relevant services in your AWS environment.

If the AWS services tab is displayed

If this you do see this tab, Audit Manager is not managing which AWS services are in scope for your assessment.

In this case, you see the following information about the services in scope that you defined:

Name	Description
AWS service	The name of the AWS service.
Category	The service category, such as *compute* or *database*.
Description	The description of the AWS service.

Audit Manager performs resource assessments for the services in this table. For example, if Amazon S3 is listed, Audit Manager can collect evidence about your S3 buckets. The exact evidence that's collected is determined by a control's data source. For instance, if the data source type is AWS Config, and the data source mapping is an AWS Config rule (such as `s3-bucket-public-write-prohibited`), Audit Manager collects the result of that rule evaluation as evidence. For more information, see What's the difference between a service in scope and a data source type? in this guide.

If your assessment was created in the console from a standard framework, Audit Manager selected the services for you and mapped their data sources according to the framework's requirements. If the standard framework contains only manual controls, no AWS services are in scope.

> **Note**
>
> The next time that you edit your assessment or change one of the custom controls in your assessment, Audit Manager takes over the management of services in scope for you. When this happens, the **AWS services** tab is removed from your assessment.

Audit owners tab

You can use this tab to see the audit owners for the assessment.

In this section, you can review the following information:

Name	Description
Audit owner	The name of the audit owner.
AWS account	The AWS account ID of the audit owner.

Tags tab

You can use this tab to see the tags for your assessment. These tags are inherited from the framework that was used to create the assessment. For more information about tags in Audit Manager, see Tagging AWS Audit Manager resources.

In this section, you can review the following information:

Name	Description
Key	The key of the tag, such as a compliance standard, regulation, or category.
Value	The value of the tag.

Changelog tab

You can use this tab to see the user activity for the assessment.

In this section, you can review the following information:

Name	Description
Date	The date of the activity.
User	The user who performed the action.
Action	The action that occurred, such as an assessment being created.
Type	The object type that changed, such as an assessment.
Resource	The resource that was affected by the change, such as the framework that the assessment was created from.

Next steps

To continue reviewing your assessment's contents, follow the steps in Reviewing an assessment control in AWS Audit Manager. This page will guide you through the assessment control details and explain the information that you see there.

Additional resources

- On my assessment details page, I'm prompted to recreate my assessment
- I can't see any controls or control sets in my assessment
- I can't see the services in scope for my assessment

Reviewing an assessment control in AWS Audit Manager

When you need to review the controls in an assessment, you'll find the information organized into several sections on the assessment control details page. These sections help you easily access and understand the relevant information for your task.

Contents

Prerequisites

The following procedure assumes that you have previously created at least one assessment. If you haven't created an assessment yet, you won't see any results when you follow these steps.

Make sure your IAM identity has appropriate permissions to view an assessment in AWS Audit Manager. Two suggested policies that grant these permissions are AWSAuditManagerAdministratorAccess and Allow users management access to AWS Audit Manager.

Procedure

To open and review an assessment control details page

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the navigation pane, choose **Assessments** and choose the name of an assessment to open it.

3. From the assessment page, choose the **Controls** tab, scroll down to the **Control sets** table, and then choose the name of a control to open it.
4. Review the assessment control details using the following information as reference.

Sections of the assessment control details page

- Control details section
- Evidence folders tab
- Details tab
- Evidence sources tab
- Comments tab
- Changelog tab

Control details section

You can use the **Control details** section to see a summary of the assessment control.

In this section, you can review the following information:

Name	Description
Description	The description that's provided for this control.
Control status	The status of the control. • **Under review** – The control hasn't been reviewed yet. Evidence is still being collected for this control, and you can add manual evidence. This is the default status. • **Reviewed** – The evidence for this control is reviewed. Evidence is still being collected, and you can add manual evidence. • **Inactive** – Automated evidence collection is stopped for this control. You can no longer add manual evidence.

Evidence folders tab

You can use this tab to see the evidence that's collected for this control. It's organized into folders on a daily basis. From here, you can also take the following actions:

- **Review an evidence folder** – To see details for any evidence folder, choose the hyperlinked folder name.
- **Add an evidence folder to an assessment report** – To include an evidence folder, select it and choose **Add to assessment report**.
- **Remove an evidence folder from an assessment report** – To exclude a folder, select it and choose **Remove from assessment report**.
- **Add manual evidence** – For instructions, see Adding manual evidence in AWS Audit Manager.

In this section, you can review the following information:

Name	Description
Evidence folder	The name of the evidence folder. The name is based on the date when the evidence was collected or manually added.
Compliance check	The number of issues in the evidence folder. This number represents the total number of security issues that were reported directly from AWS Security Hub, AWS Config, or both. If you see **Not applicable**, this indicates that you either don't have Security Hub or AWS Config enabled, or the evidence comes from a different data source type.
Total evidence	The total number of evidence items inside the folder.
Assessment report selection	The number of evidence items within the folder that are included in the assessment report.

Tip

If you can't see the evidence folder that you're looking for, change the dropdown filter to **All time**. Otherwise, you'll see the last seven days of folders by default.

Details tab

In this section, you can review the following information:

Name	Description
Testing information	The recommended procedure to test that the control is working as intended.
Action plan	The recommended actions to take if the control needs to be remediated.

Evidence sources tab

You can use this tab to see where the assessment control collects evidence from. The evidence sources can include any of the following:

Name	Description
Common controls	These are the common controls that collect evidence to support the assessment control. Common controls collect evidence using underlying data sources that AWS manages for you. For every common control that's listed, Audit Manager collects the relevant evidence for all of the supporting core controls. Choose a common control to see the related core controls.
Core controls	These are the core controls that collect evidence to support the assessment control. Core controls collect evidence by using a predefined group of data sources that AWS manages for you. Choose a core control to see the underlying data sources.
Data sources	These are the individual data sources that collect evidence to support the assessment control. • **Name** – The name of the data source. • **Type** – The type of data source that the evidence comes from. • If Audit Manager collects the evidence, the type can be *AWS Security Hub*, *AWS Config*, *AWS CloudTrail*, or *AWS API calls*.

Name	Description

	• If you upload your own evidence, the type is *Manual*. A description indicates if the required manual evidence is a *File upload* or a *Text response*.
	• **Mapping** – The specific keyword that's used to collect evidence.
	  • If the type is *AWS Config*, the mapping is an AWS Config rule (such as `SNS_ENCRYPTED_KMS`)
	  • If the type is *AWS Security Hub*, the mapping is a Security Hub control (such as `EC2.1`).
	  • If the type is *AWS API calls*, the mapping is an API call (such as `kms_ListKeys`).
	  • If the type is *AWS CloudTrail*, the mapping is a CloudTrail event (such as `CreateAccessKey`).
	• **Frequency** – How often Audit Manager collects evidence for an AWS API call data source.

Comments tab

In this tab, you can add a comment about the control and its evidence. You can also see a list of previous comments.

- Under **Send comments**, you can add comments for a control by entering text and then choosing **Submit comments**.
- Under **Previous comments**, you can view a list of previous comments along with the date the comment was made and the associated user ID.

Changelog tab

You can use this tab to see the user activity for the assessment control. The same information is available as audit trail logs in AWS CloudTrail. With the user activity that's captured directly in Audit Manager, you can easily review an audit trail of activity for a given control.

In this section, you can review the following information:

Name	Description
Date	The date and time of the activity, represented in Coordinated Universal Time (UTC).
User	The user or role that performed the activity.
Action	The action that occurred, such as an assessment being created.
Type	The object type that changed, such as an assessment.
Resource	The resource that was affected by the change, such as the framework that the assessment was created from.

Audit Manager tracks the following user activity in changelogs:

- Creating an assessment
- Editing an assessment
- Completing an assessment
- Deleting an assessment
- Delegating a control set for review
- Submitting a reviewed control set back to the audit owner
- Uploading manual evidence
- Updating a control status
- Generating assessment reports

Next steps

To continue reviewing your assessment, follow the steps in Reviewing an evidence folder in AWS Audit Manager. This page will guide you through the evidence folders and show you how to understand the information that you see.

Additional resources

- I can't see any controls or control sets in my assessment

Reviewing an evidence folder in AWS Audit Manager

As your assessment collects evidence, Audit Manager organizes it into folders for your convenience. When you need to review an evidence folder, you'll find the information organized into several sections.

Contents

Prerequisites

The following procedure assumes that you have previously created at least one assessment. If you haven't created an assessment yet, you won't see any results when you follow these steps.

Make sure your IAM identity has appropriate permissions to view an assessment in AWS Audit Manager. Two suggested policies that grant these permissions are AWSAuditManagerAdministratorAccess and Allow users management access to AWS Audit Manager.

Keep in mind that it takes up to 24 hours for an assessment to start collecting automated evidence. If your assessment has no evidence yet, you won't see any results when you follow these steps.

Procedure

To open and review an evidence folder

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the navigation pane, choose **Assessments**, and then choose an assessment.
3. From the assessment page, choose the **Controls** tab, scroll down to the **Controls** table, and then choose an assessment control.

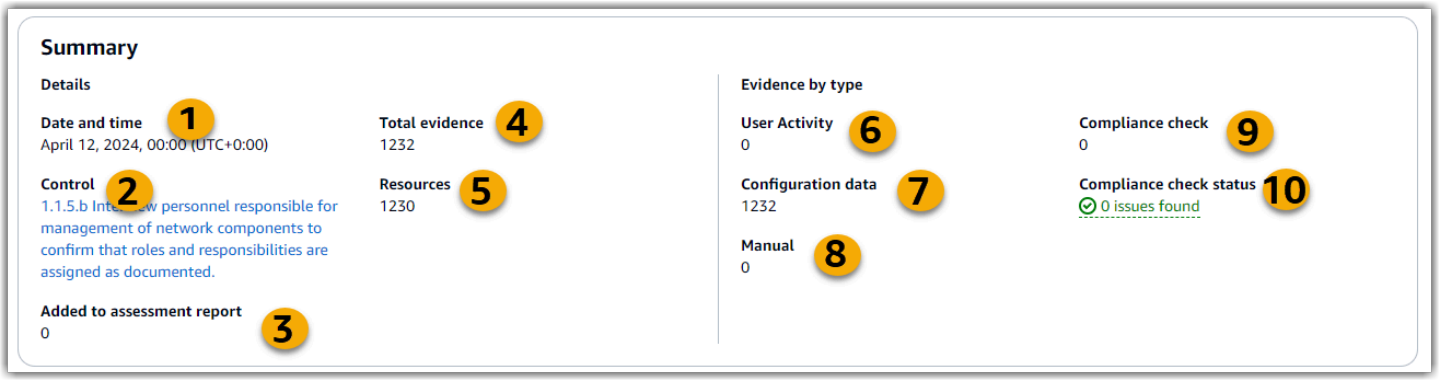
4. From the assessment control page, choose the **Evidence folders** tab.
5. In the **Evidence folders** table, choose the name of an evidence folder.
6. Review the evidence folder using the following information as reference.

Sections of an evidence folder page

- Evidence folder summary
- Evidence table

Evidence folder summary

You can use the **Summary** section of the page to see a high-level overview of the evidence in the evidence folder. To learn more about different evidence types, see Evidence.



In this section, you can review the following information:

Name	Description
1. Date and time	The time and date when the evidence folder was created. This is represented in Coordinated Universal Time (UTC).
2. Control	The name of the control that's related the evidence folder.
3. Added to assessment report	The number of evidence items that were selected to be included in the assessment report.
4. Total evidence	The total number of evidence items in the evidence folder.
5. Resources	The total number of AWS resources that were assessed when collecting the evidence in this folder.

Name	Description
6. User activity	The number of evidence items that fall under the *user activity* category. This evidence is collected from AWS CloudTrail logs.
7. Configuration data	The number of evidence items that fall under the *configuration data* category. This evidence is collected from API calls that take configuration snapshots of other AWS services.
8. Manual	The number of evidence items that fall under the *manual* category. This evidence is added manually.
9. Compliance check	The number of evidence items that fall under the *compliance check* category. This evidence is collected from AWS Config, AWS Security Hub, or both.
10. Compliance check status	The total number of issues that were reported directly from AWS Security Hub, AWS Config, or both.

Evidence table

You can use the **Evidence** table to see the evidence that's contained within the evidence folder. From here table, you can also take the following actions:

- **Review individual evidence** – To see details for any piece of evidence, choose the hyperlinked evidence name under the **Time** column.
- **Add evidence to an assessment report** – To include evidence, select it and choose **Add to assessment report**.
- **Remove evidence from an assessment report** – To exclude evidence, select it and choose **Remove from assessment report**.
- **Add manual evidence** – For instructions, see Adding manual evidence in AWS Audit Manager.

In this table, you can review the following information:

Name	Description
Time	Specifies when the evidence was collected. This also serves as the name of the evidence. The time is represented in Coordinated Universal Time (UTC).
Compliance check	The evaluation status for evidence that falls under the *compliance check* category. • For evidence that's collected from Security Hub, a **Pass** or **Fail** result is reported directly from Security Hub. • For evidence that's collected from AWS Config, a **Compliant** or **Non-compliant** result is reported directly from AWS Config. • If **Not applicable** is shown, this indicates that you either don't have AWS Config or Security Hub enabled, or the evidence comes from a different data source type.
Evidence by type	The type of evidence. • **Compliance check** evidence is collected from AWS Config or AWS Security Hub. • **User activity** evidence is collected from AWS CloudTrail. • **Configuration data** evidence is collected from API calls to other AWS services. • **Manual** evidence is evidence that you add manually.
Data source	The data source where the evidence is collected from.
Event name	The name of the event that invoked the evidence collection.
Event source	The service principal that identifies the relevant AWS service for the event.
Resources	The number of resources that were assessed when collecting the evidence.
Assessment report selection	Indicates whether the evidence is included in the assessment report.

Name	Description
	• To include evidence, select the evidence and choose **Add to assessment report**. • To exclude evidence, select the evidence and choose **Remove from assessment report**.

Next steps

When you're ready to explore the individual pieces of evidence in a folder, follow the steps in Reviewing evidence in AWS Audit Manager. This page will guide you through the evidence details and how to interpret the information that you see there.

Additional resources

- For solutions to evidence issues in Audit Manager, see Troubleshooting assessment and evidence collection issues.

Reviewing evidence in AWS Audit Manager

When you need to review a specific piece of evidence, follow the instructions on this page. You'll find the evidence details organized into several sections.

Contents

Prerequisites

The following procedure assumes that you have previously created at least one assessment. If you haven’t created an assessment yet, you won’t see any results when you follow these steps.

Make sure your IAM identity has appropriate permissions to view an assessment in AWS Audit Manager. Two suggested policies that grant these permissions are AWSAuditManagerAdministratorAccess and Allow users management access to AWS Audit Manager.

Keep in mind that it takes up to 24 hours for an assessment to start collecting automated evidence. If your assessment has no evidence yet, you won't see any results when you follow these steps.

Procedure

To open and review an evidence details page

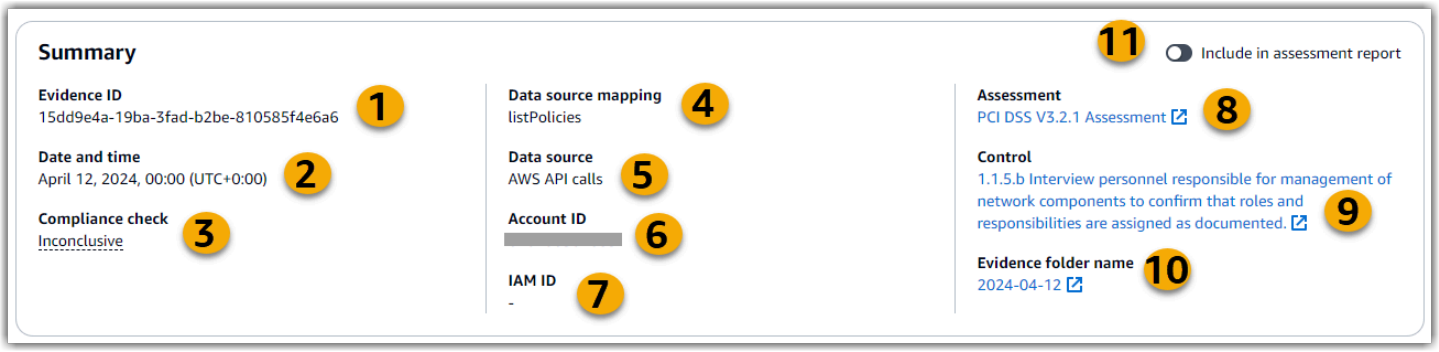
1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the navigation pane, choose **Assessments**, and then choose an assessment.
3. From the assessment page, choose the **Controls** tab, scroll down to the **Controls** table, and then choose a control.
4. From the control page, choose the **Evidence folders** tab.
5. In the **Evidence folders** table, choose the name of an evidence folder.
6. Choose the evidence name under the **Time** column to open the evidence details page.
7. Review the evidence details using the following information as reference.

Sections of an evidence details page

- Summary
- Attributes
- Resources included

Summary

You can use the **Summary** section to see an overview of the evidence.



In this section, you can review the following information:

Name	Description
1. Evidence ID	The unique identifier for the evidence.
2. Date and time	The time and date when the evidence was collected. This is represented in Coordinated Universal Time (UTC).
3. Compliance check	The evaluation status for compliance check evidence. • For evidence that's collected from AWS Security Hub, a **Pass** or **Fail** result is reported directly from AWS Security Hub. • For evidence that's collected from AWS Config, a **Compliant** or **Non-compliant** result is reported directly from AWS Config. • If **Not applicable** is shown, this indicates one of two things. Either you don't have AWS Security Hub or AWS Config enabled. Or, the evidence comes from a different data source.
4. Data source mapping	The mapping keyword that was used to collect the evidence.
5. Data source type	The type of data source where the evidence was collected from.
6. Account ID	The AWS account that's associated with the evidence.
7. IAM ID	The relevant user or role, if applicable.
8. Assessment	The name of the assessment that's associated with the evidence.
9. Control	The name of the control that's associated with the evidence.

Name	Description
10. Evidence folder name	The name of the evidence folder that contains the evidence.
11. Include in assessment report	The switch that enables you to include or exclude the evidence from the assessment report.

Attributes

You can use the **Attributes** table to see the evidence attributes in detail.

In this table, you can review the following information:

Name	Description
Attribute name	The key for the attribute.
Value	The value of the attribute. In some cases, a link to a JSON file is provided with more information.

Resources included

You can use the **Resources included** table to see the resources that were assessed to generate this evidence.

In this section, you can review the following information:

Name	Description
ARN	The Amazon Resource Name (ARN) of the resource. An ARN might not be available for all evidence types.
Resource compliance	The evaluation status for the resource. • For evidence that's collected from AWS Security Hub, a **Pass** or **Fail** result is reported directly from Security Hub. • For evidence that's collected from AWS Config, a **Compliant** or **Non-compliant** result is reported directly from AWS Config.

Name	Description
	• If **Not applicable** is shown, this indicates that you either don't have AWS Config or Security Hub enabled, or the evidence comes from a different data source.
Value	More information about the resource assessment. In some cases, a link to a JSON file is provided with more information.

Additional resources

- For solutions to evidence issues in Audit Manager, see Troubleshooting assessment and evidence collection issues.

Editing an assessment in AWS Audit Manager

You might encounter situations where you need to edit your existing assessments in AWS Audit Manager. Perhaps the scope of your audit has changed, requiring updates to the AWS accounts included in the assessment. Or, you might need to revise the list of audit owners assigned to the assessment due to personnel changes. In such cases, you can edit your active assessments and make necessary adjustments without disrupting your evidence collection.

The following page outlines the steps to edit your assessment details, change the AWS accounts in scope, update the audit owners, and review and save your changes.

Prerequisites

The following procedure assumes that you have previously created at least one assessment, and it is in an active state.

Make sure your IAM identity has appropriate permissions to edit an assessment in AWS Audit Manager. Two suggested policies that grant these permissions are AWSAuditManagerAdministratorAccess and Allow users management access to AWS Audit Manager.

Procedure

Tasks

Step 1: Edit assessment details

Follow these steps to edit the details of your assessment.

To edit an assessment

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the navigation pane, choose **Assessments**.
3. Select an assessment, and choose **Edit**.
4. Under **Edit assessment details**, edit your assessment details as needed.
5. Choose **Next**.

Step 2: Edit AWS accounts in scope

In this step, you can change which accounts are included in your assessment. Audit Manager can support up to 200 accounts in the scope of an assessment, and 250 unique member accounts across all assessments.

To edit AWS accounts in scope

1. To add an AWS account, select the check box next to the account name.
2. To remove an AWS account, clear the check box next to the account name.
3. Choose **Next**.

> **Note**
>
> To edit the delegated administrator for Audit Manager, see Changing a delegated administrator.

Step 3: Edit audit owners

In this step, you can change which audit owners are included in your assessment.

To edit audit owners

1. To add an audit owner, select the check box next to the account name.
2. To remove an audit owner, clear the check box next to the account name.
3. Choose **Next**.

Audit owner permissions

The below policy is attached for all the audit owners of an assessment.

Audit Manager replaces the *placeholder text* with your account and resource identifiers before attaching the policy.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditOwner",
            "Effect": "Allow",
            "Principal": {
                "AWS": "Principal for user/role who are the audit owners of the
 Assessment"
            },
            "Action": [
                "auditmanager:GetAssessment",
                "auditmanager:UpdateAssessment",
                "auditmanager:UpdateAssessmentControlSetStatus",
                "auditmanager:UpdateAssessmentStatus",
                "auditmanager:UpdateAssessmentControl",
                "auditmanager:DeleteAssessment",
                "auditmanager:GetChangeLogs",
                "auditmanager:GetEvidenceFoldersByAssessment",
                "auditmanager:GetEvidenceFoldersByAssessmentControl",
                "auditmanager:BatchImportEvidenceToAssessmentControl",
                "auditmanager:GetEvidenceFolder",
```

```
                "auditmanager:GetEvidence",
                "auditmanager:GetEvidenceByEvidenceFolder",
                "auditmanager:BatchCreateDelegationByAssessment",
                "auditmanager:BatchDeleteDelegationByAssessment",
                "auditmanager:AssociateAssessmentReportEvidenceFolder",
                "auditmanager:BatchAssociateAssessmentReportEvidence",
                "auditmanager:BatchDisassociateAssessmentReportEvidence",
                "auditmanager:CreateAssessmentReport",
                "auditmanager:DeleteAssessmentReport",
                "auditmanager:DisassociateAssessmentReportEvidenceFolder",
                "auditmanager:GetAssessmentReportUrl"
            ],
            "Resource": [
                "arn:aws:auditmanager:us-
east-1:123456789012:assessment/assessment_ID",
                "arn:aws:auditmanager:us-
east-1:123456789012:assessment/assessment_ID/*"
            ]
        }
    ]
}
```

Step 4: Review and save

Review the information for your assessment. To change the information for a step, choose **Edit**. When you're finished, choose **Save changes** to confirm your edits.

After you complete your edits, the changes to the assessment take effect at 00:00 UTC the following day.

Next steps

When you no longer need to collect evidence for a specific assessment control, you can change the status of that control. For instructions, see Changing the status of an assessment control in AWS Audit Manager.

When you no longer need to collect evidence for the entire assessment, you can change the assessment status to inactive. For instructions, see Changing the status of an assessment to inactive in AWS Audit Manager.

Additional resources

- For solutions to assessment issues in Audit Manager, see Troubleshooting assessment and evidence collection issues.
- For information about why it's no longer possible to edit services in scope, see I can't edit the services in scope for my assessment in the *Troubleshooting* section of this guide.

Adding manual evidence in AWS Audit Manager

Audit Manager can automatically collect evidence for many controls. However, some controls might require evidence that can't be collected automatically. In such cases, you can manually add your own evidence.

Consider the following examples:

- Some controls relate to the provision of physical records (such as signatures), or events that aren’t generated in the cloud (such as observations and interviews). In these cases, you can manually add files as evidence. For instance, if a control requires information about your organizational structure, you can upload a copy of your company’s org chart as manual evidence.
- Some controls represent a vendor risk assessment question. A risk assessment question might require documentation as evidence (such as an org chart). Or, it might only need a simple text response (such as a list of job titles). For the latter, you can respond to the question and save your response as manual evidence.

You can also use the manual upload feature to manage evidence from multiple environments. If your company uses a hybrid cloud model or multicloud model, you can upload evidence from your on-premises environment, an environment hosted in the cloud, or your SaaS applications. This enables you to organize your evidence (regardless of where it came from) by storing it within the structure of an Audit Manager assessment, where each piece of evidence is mapped to a specific control.

Key points

When it comes to adding manual evidence to your assessments in Audit Manager, you have three methods to choose from.

1. **Importing a file from Amazon S3 -** This method is ideal when you have evidence files stored in an S3 bucket, such as documentation, reports, or other artifacts that can't be automatically collected by Audit Manager. By importing these files directly from S3, you can seamlessly integrate this manual evidence with the automatically collected evidence.
2. **Uploading a file from your browser** - If you have evidence files locally stored on your computer or network, you can manually upload them to Audit Manager using this method. This approach is particularly useful when you need to include physical records, such as scanned documents or images, that aren't available in digital format within your AWS environment.
3. **Adding free-form text as evidence** - In some cases, the evidence you need to provide is not in the form of a file but rather a text response or explanation. This method allows you to enter free-form text directly into Audit Manager. This can be especially helpful when responding to vendor risk assessment questions.

Additional resources

- For instructions on how to add manual evidence to an assessment control, see the following resources. Keep in mind you can only use one method at a time.
  - Importing manual evidence files from Amazon S3
  - Uploading manual evidence files from your browser
  - Entering free-form text responses as manual evidence
- To learn which file formats you can use, see Supported file formats for manual evidence.
- To learn more about the different types of evidence in Audit Manager, see evidence in the *Concepts and terminology* section of this guide.
- For troubleshooting assistance, see I can’t upload manual evidence to a control.

Importing manual evidence files from Amazon S3

You can manually import evidence files from an Amazon S3 bucket into your assessment. This enables you to supplement the automatically collected evidence with additional supporting materials.

Prerequisites

- The maximum supported size for a single manual evidence file is 100 MB.

- You must use one of the Supported file formats for manual evidence.
- Each AWS account can manually upload up to 100 evidence files to a control each day. Exceeding this daily quota causes any additional manual uploads to fail for that control. If you need to upload a large amount of manual evidence to a single control, upload your evidence in batches across several days.
- When a control is *inactive*, you can't add manual evidence to that control. To add manual evidence, you must first change the control status to either *under review* or *reviewed*.
- Make sure your IAM identity has appropriate permissions to manage an assessment in AWS Audit Manager. Two suggested policies that grant these permissions are AWSAuditManagerAdministratorAccess and Allow users management access to AWS Audit Manager.

Procedure

You can import a file using the Audit Manager console, the Audit Manager API, or the AWS Command Line Interface (AWS CLI).

AWS console

> **Important**
>
> We strongly recommend that you never import any sensitive or personally identifiable information (PII) as manual evidence. This includes, but is not limited to, Social Security numbers, addresses, phone numbers, or any other information that could be used to identify an individual.

To import a file from S3 on the Audit Manager console

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the left navigation pane, choose **Assessments** and then choose an assessment.
3. Choose the **Controls** tab, scroll down to **Control sets** and then choose a control.
4. On the **Evidence folders** tab, choose **Add manual evidence**, and then choose **Import file from S3**.

5. On the next page, enter the S3 URI of the evidence. You can find the S3 URI by navigating to the object in the Amazon S3 console and choosing **Copy S3 URI**.
6. Choose **Upload**.

AWS CLI

> **Important**
>
> We strongly recommend that you never import any sensitive or personally identifiable information (PII) as manual evidence. This includes, but is not limited to, Social Security numbers, addresses, phone numbers, or any other information that could be used to identify an individual.

In the following procedure, replace the *placeholder text* with your own information.

To import a file from S3 in the AWS CLI

1. Run the `list-assessments` command to see a list of your assessments.

   ```
   aws auditmanager list-assessments
   ```

   In the response, find the assessment that you want to upload evidence to and take note of the assessment ID.
2. Run the `get-assessment` command and specify the assessment ID from step one.

   ```
   aws auditmanager get-assessment --assessment-
   id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
   ```

   In the response, find the control set and the control that you want to upload evidence to, and take note of their IDs.
3. Run the `batch-import-evidence-to-assessment-control` command with the following parameters:

   - `--assessment-id` – Use the assessment ID from step one.
   - `--control-set-id` – Use the control set ID from step two.
   - `--control-id` – Use the control ID from step two.

- `--manual-evidence` – Use `s3ResourcePath` as the manual evidence type and specify the S3 URI of the evidence. You can find the S3 URI by navigating to the object in the Amazon S3 console and choosing **Copy S3 URI**.

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet --control-
id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence s3ResourcePath=s3://
amzn-s3-demo-bucket/EXAMPLE-FILE.extension
```

Audit Manager API

> **Important**
>
> We strongly recommend that you never import any sensitive or personally identifiable information (PII) as manual evidence. This includes, but is not limited to, Social Security numbers, addresses, phone numbers, or any other information that could be used to identify an individual.

To import a file from S3 using the API

1. Call the `ListAssessments` operation to see a list of your assessments. In the response, find the assessment that you want to upload evidence to and take note of the assessment ID.
2. Call the `GetAssessment` operation and specify the assessment ID from step one. In the response, find the control set and the control that you want to upload evidence to, and take note of their IDs.
3. Call the `BatchImportEvidenceToAssessmentControl` operation with the following parameters:

   - `assessmentId` – Use the assessment ID from step one.
   - `controlSetId` – Use the control set ID from step two.
   - `controlId` – Use the control ID from step two.
   - `manualEvidence` – Use `s3ResourcePath` as the manual evidence type and specify the S3 URI of the evidence. You can find the S3 URI by navigating to the object in the Amazon S3 console and choosing **Copy S3 URI**.

For more information, choose any of the links in the previous procedure to read more in the *AWS Audit Manager API Reference*. This includes information about how to use these operations and parameters in one of the language-specific AWS SDKs.

Next steps

After you've added and reviewed the evidence for your assessment, you can generate an assessment report. For more information, see Preparing an assessment report in AWS Audit Manager.

Additional resources

To learn which file formats you can use, see Supported file formats for manual evidence.

Uploading manual evidence files from your browser

You can manually upload evidence files from your browser into your Audit Manager assessment. This enables you to supplement the automatically collected evidence with additional supporting materials.

Prerequisites

- The maximum supported size for a single manual evidence file is 100 MB.
- You must use one of the Supported file formats for manual evidence.
- Each AWS account can manually upload up to 100 evidence files to a control each day. Exceeding this daily quota causes any additional manual uploads to fail for that control. If you need to upload a large amount of manual evidence to a single control, upload your evidence in batches across several days.
- When a control is *inactive*, you can't add manual evidence to that control. To add manual evidence, you must first change the control status to either *under review* or *reviewed*.
- Make sure your IAM identity has appropriate permissions to manage an assessment in AWS Audit Manager. Two suggested policies that grant these permissions are AWSAuditManagerAdministratorAccess and Allow users management access to AWS Audit Manager.

Procedure

You can upload a file using the Audit Manager console, the Audit Manager API, or the AWS Command Line Interface (AWS CLI).

AWS console

> **Important**
>
> We strongly recommend that you never upload any sensitive or personally identifiable information (PII) as manual evidence. This includes, but is not limited to, Social Security numbers, addresses, phone numbers, or any other information that could be used to identify an individual.

To upload a file from your browser on the Audit Manager console

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the left navigation pane, choose **Assessments** and then choose an assessment.
3. On the **Controls** tab, scroll down to **Control sets** and then choose a control.
4. From the **Evidence folders** tab, choose **Add manual evidence**.
5. Choose **Upload file from browser**.
6. Choose the file that you want to upload.
7. Choose **Upload**.

AWS CLI

> **Important**
>
> We strongly recommend that you never upload any sensitive or personally identifiable information (PII) as manual evidence. This includes, but is not limited to, Social Security numbers, addresses, phone numbers, or any other information that could be used to identify an individual.

In the following procedure, replace the *`placeholder text`* with your own information.

To upload a file from your browser in the AWS CLI

1. Run the `list-assessments` command to see a list of your assessments.

```
aws auditmanager list-assessments
```

   In the response, find the assessment that you want to upload evidence to and take note of the assessment ID.

2. Run the `get-assessment` command and specify the assessment ID from step one.

```
aws auditmanager get-assessment --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

   In the response, find the control set and the control that you want to upload evidence to, and take note of their IDs.

3. Run the `get-evidence-file-upload-url` command and specify the file that you want to upload.

```
aws auditmanager get-evidence-file-upload-url --file-name fileName.extension
```

   In the response, take note of the presigned URL and the `evidenceFileName`.

4. Use the presigned URL from step three to upload the file from your browser. This action uploads your file to Amazon S3, where it's saved as an object that can be attached to an assessment control. In the following step, you'll reference the newly-created object by using the `evidenceFileName` parameter.

> **Note**
>
> When you upload a file using a presigned URL, Audit Manager protects and stores your data by using server side encryption with AWS Key Management Service. To support this, you must use the `x-amz-server-side-encryption` header in your request when you use the presigned URL to upload your file.
> If you're using a customer managed AWS KMS key in your Audit Manager Configuring your data encryption settings settings, make sure that you also include the `x-amz-server-side-encryption-aws-kms-key-id` header in your request. If the `x-amz-server-side-encryption-aws-kms-key-id` header isn't

present in the request, Amazon S3 assumes that you want to use the AWS managed key.
For more information, see Protecting data using server-side encryption with AWS Key Management Service keys (SSE-KMS) in the *Amazon Simple Storage Service User Guide*.

5. Run the `batch-import-evidence-to-assessment-control` command with the following parameters:

   - `--assessment-id` – Use the assessment ID from step one.
   - `--control-set-id` – Use the control set ID from step two.
   - `--control-id` – Use the control ID from step two.
   - `--manual-evidence` – Use `evidenceFileName` as the manual evidence type and specify the evidence file name from step three.

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet
 --control-id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence
 evidenceFileName=fileName.extension
```

Audit Manager API

Important

We strongly recommend that you never upload any sensitive or personally identifiable information (PII) as manual evidence. This includes, but is not limited to, Social Security numbers, addresses, phone numbers, or any other information that could be used to identify an individual.

To upload a file from your browser using the API

1. Call the `ListAssessments` operation. In the response, find the assessment that you want to upload evidence to and take note of the assessment ID.

2. Call the `GetAssessment` operation and specify the `assessmentId` from step one. In the response, find the control set and the control that you want to upload evidence to, and take note of their IDs.
3. Call the `GetEvidenceFileUploadUrl` operation and specify the `fileName` that you want to upload. In the response, take note of the presigned URL and the `evidenceFileName`.
4. Use the presigned URL from step three to upload the file from your browser. This action uploads your file to Amazon S3, where it's saved as an object that can be attached to an assessment control. In the following step, you'll reference the newly-created object by using the `evidenceFileName` parameter.

   > **Note**
   >
   > When you upload a file using a presigned URL, Audit Manager protects and stores your data by using server side encryption with AWS Key Management Service. To support this, you must use the `x-amz-server-side-encryption` header in your request when you use the presigned URL to upload your file.
   > If you're using a customer managed AWS KMS key in your Audit Manager Configuring your data encryption settings settings, make sure that you also include the `x-amz-server-side-encryption-aws-kms-key-id` header in your request. If the `x-amz-server-side-encryption-aws-kms-key-id` header isn't present in the request, Amazon S3 assumes that you want to use the AWS managed key.
   > For more information, see Protecting data using server-side encryption with AWS Key Management Service keys (SSE-KMS) in the *Amazon Simple Storage Service User Guide*.

5. Call the `BatchImportEvidenceToAssessmentControl` operation with the following parameters:

   - `assessmentId` – Use the assessment ID from step one.
   - `controlSetId` – Use the control set ID from step two.
   - `controlId` – Use the control ID from step two.
   - `manualEvidence` – Use `evidenceFileName` as the manual evidence type and specify the evidence file name from step three.

For more information, choose any of the links in the previous procedure to read more in the *AWS Audit Manager API Reference*. This includes information about how to use these operations and parameters in one of the language-specific AWS SDKs.

Next steps

After you've collected and reviewed the evidence for your assessment, you can generate an assessment report. For more information, see Preparing an assessment report in AWS Audit Manager.

Additional resources

To learn which file formats you can use, see Supported file formats for manual evidence.

Entering free-form text responses as manual evidence

You can provide additional context and supporting information for an assessment control by entering free-form text and saving that text as evidence. This allows you to manually document details that aren't captured through automatic evidence collection.

For example, you can use Audit Manager to create custom controls that represent questions in a vendor risk assessment questionnaire. In this case, the name of each control is a specific question that asks for information about your organization's security and compliance posture. To record your response to a given vendor risk assessment question, you can enter a text response and save it as manual evidence for the control.

Prerequisites

- When a control is *inactive*, you can't add manual evidence to that control. To add manual evidence, you must first change the control status to either *under review* or *reviewed*.
- Make sure your IAM identity has appropriate permissions to manage an assessment in AWS Audit Manager. Two suggested policies that grant these permissions are AWSAuditManagerAdministratorAccess and Allow users management access to AWS Audit Manager.

Procedure

You can enter text responses using the Audit Manager console, the Audit Manager API, or the AWS Command Line Interface (AWS CLI).

AWS console

> **Important**
>
> We strongly recommend that you never enter any sensitive or personally identifiable information (PII) as manual evidence. This includes, but is not limited to, Social Security numbers, addresses, phone numbers, or any other information that could be used to identify an individual.

To enter a text response on the Audit Manager console

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the left navigation pane, choose **Assessments** and then choose an assessment.
3. Choose the **Controls** tab, scroll down to **Control sets** and then choose a control.
4. From the **Evidence folders** tab, choose **Add manual evidence**.
5. Choose **Enter text response**.
6. In the pop-up window that appears, enter your response in plain text format.
7. Choose **Confirm**.

AWS CLI

> **Important**
>
> We strongly recommend that you never enter any sensitive or personally identifiable information (PII) as manual evidence. This includes, but is not limited to, Social Security numbers, addresses, phone numbers, or any other information that could be used to identify an individual.

In the following procedure, replace the *`placeholder text`* with your own information.

To enter a text response in the AWS CLI

1. Run the `list-assessments` command.

```
aws auditmanager list-assessments
```

   In the response, find the assessment that you want to upload evidence to and take note of the assessment ID.

2. Run the `get-assessment` command and specify the assessment ID from step one.

```
aws auditmanager get-assessment --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

   In the response, find the control set and control that you want to upload evidence to, and take note of their IDs.

3. Run the `batch-import-evidence-to-assessment-control` command with the following parameters:

   - `--assessment-id` – Use the assessment ID from step one.
   - `--control-set-id` – Use the control set ID from step two.
   - `--control-id` – Use the control ID from step two.
   - `--manual-evidence` – Use `textResponse` as the manual evidence type and enter the text that you want to save as manual evidence.

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet --control-
id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence textResponse="enter
 text here"
```

Audit Manager API

> **Important**
>
> We strongly recommend that you never enter any sensitive or personally identifiable information (PII) as manual evidence. This includes, but is not limited to, Social Security

numbers, addresses, phone numbers, or any other information that could be used to identify an individual.

To enter a text response using the API

1. Call the `ListAssessments` operation. In the response, find the assessment that you want to upload evidence to and take note of the assessment ID.
2. Call the `GetAssessment` operation and specify the `assessmentId` from step one. In the response, find the control set and control that you want to upload evidence to, and take note of their IDs.
3. Call the `BatchImportEvidenceToAssessmentControl` operation with the following parameters:
   - `assessmentId` – Use the assessment ID from step one.
   - `controlSetId` – Use the control set ID from step two.
   - `controlId` – Use the control ID from step two.
   - `manualEvidence` – Use `textResponse` as the manual evidence type and enter the text that you want to save as manual evidence.

For more information, choose any of the links in the previous procedure to read more in the *AWS Audit Manager API Reference*. This includes information about how to use these operations and parameters in one of the language-specific AWS SDKs.

Next steps

After you've collected and reviewed the evidence for your assessment, you can generate an assessment report. For more information, see Preparing an assessment report in AWS Audit Manager.

Supported file formats for manual evidence

The following table lists and describes the types of file that you can upload as manual evidence. For each file type, the table also lists the supported file extensions.

File type	Description	Supported file extensions
Compression or archive	GNU Zip compressed archives and ZIP compressed archives	`.gz`, `.zip`
Document	Common document files such as PDFs and Microsoft Office files	`.doc`, `.docx`, `.pdf`, `.ppt`, `.pptx`, `.xls`, `.xlsx`
Image	Image and graphic files	`.jpeg`, `.jpg`, `.png`, `.svg`
Text	Other non-binary text files, such as plain-text documents and markup language files	`.cer`, `.csv`, `.html`, `.jmx`, `.json`, `.md`, `.out`, `.rtf`, `.txt`, `.xml`, `.yaml`, `.yml`

Additional resources

Review the following pages to learn about the different ways that you can add your own evidence to an assessment control.

- Importing manual evidence files from Amazon S3
- Uploading manual evidence files from your browser
- Entering free-form text responses as manual evidence

Preparing an assessment report in AWS Audit Manager

After you've collected and reviewed the evidence for your assessment, you can generate an assessment report. An assessment report summarizes your assessment and provides links to an organized set of folders that contain the related evidence.

Key points

Newly-collected evidence doesn't automatically appear in an assessment report. This means that you can control which evidence you want to include in the report. After you select the evidence that you want to include, you can generate the final assessment report to share with your auditors.

When you generate an assessment report, it's placed into the S3 bucket that you chose as your assessment report destination. You can also download the assessment report from the download center in Audit Manager.

Additional resources

For more information about assessment reports and how to manage them, see the following resources.

- Adding evidence to an assessment report
- Removing evidence from an assessment report
- Generating an assessment report
- Downloading an assessment report
- Navigating an assessment report and exploring its contents
- Validating an assessment report
- Deleting an assessment report
- Generating assessment reports from your evidence finder search results
- Configuring your default assessment report destination
- Troubleshooting assessment report issues

Adding evidence to an assessment report

Before you can generate an assessment report, you must add at least one piece of evidence to your assessment report. You can either add an entire evidence folder, or you can add specific evidence items from within a folder.

Procedure

To include evidence in an assessment report, follow these steps.

To add evidence to an assessment report

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the navigation pane, choose **Assessments** and then choose an assessment.
3. On the **Controls** tab, scroll down to the **Control sets** table and choose a control with evidence that you want to include in the assessment report.
4. Choose how you want to add evidence to your assessment report.

   a. To add an entire evidence folder, scroll down to **Evidence folders**, select the folder that you want to add, and then choose **Add to assessment report**.

   > **Tip**
   >
   > If you can't see the folder that you're looking for, change the dropdown filter to **All time**. Otherwise, you'll see the last seven days of folders by default.
   > If **Add to assessment report** is greyed out, the evidence folder was already added to the assessment report.

   b. To add specific evidence, choose an evidence folder to open its contents. Select one or more items from the list, and then choose **Add to assessment report**.

   > **Tip**
   >
   > If **Add to assessment report** is greyed out, make sure that you selected the check box next to the evidence, and then try again.

5. After you add the evidence to the assessment report, a green success banner appears. Choose **View evidence in assessment report** to see the evidence that will be included in your assessment report.
   - Alternatively, you can see the evidence that will be included in your assessment report by navigating back to your assessment and choosing the **Assessment report selection** tab.

Next steps

If you need to remove evidence from an assessment report, see Removing evidence from an assessment report.

When you're ready to generate an assessment report, see Generating an assessment report.

Additional resources

To find answers to common questions and issues, see Troubleshooting assessment report issues in the *Troubleshooting* section of this guide.

Removing evidence from an assessment report

If you need to remove evidence from an assessment report, follow these steps. You can either remove an entire evidence folder, or you can remove specific evidence items from within a folder.

Procedure

To remove evidence from an assessment report

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the navigation pane, choose **Assessments** and then choose the name of the assessment to open it.
3. On the **Controls** tab, scroll down to the **Control sets** table and choose the name of a control to open it.
4. Choose how you want to remove evidence from your assessment report.

    a. To remove an entire evidence folder, scroll down to **Evidence folders**, select the folder that you want to remove, and then choose **Remove from assessment report**.

    > **Tip**
    >
    > If you can't see the folder that you're looking for, change the dropdown filter to **All time**. Otherwise, you'll see the last seven days of folders by default.
    > If **Remove from assessment report** is greyed out, the evidence folder was already removed from the assessment report.

    b. To remove specific evidence, choose an evidence folder to open its contents. Select one or more items from the list, and then choose **Remove from assessment report**.

> **Tip**
>
> If **Remove from assessment report** is greyed out, make sure that you selected the check box next to the evidence, and then try again.

5. After you add the evidence to the assessment report, a green success banner appears. Choose **View evidence in assessment report** to see the evidence that will be included in your assessment report.
   - Alternatively, you can see the evidence that will be included in your assessment report by navigating back to your assessment and choosing the **Assessment report selection** tab.

Next steps

When you're ready to generate an assessment report, see Generating an assessment report.

Additional resources

To find answers to common questions and issues, see Troubleshooting assessment report issues in the *Troubleshooting* section of this guide.

Generating an assessment report

When you're ready to generate your assessment report, follow these steps.

Prerequisites

Before you can generate an assessment report, you must add at least one piece of evidence to your assessment report. You can either add an entire evidence folder, or you can add individual evidence items from within a folder.

To ensure that your assessment report is generated successfully, review our Configuration tips for your assessment report destination.

Procedure

To generate an assessment report

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.

2. In the left navigation pane, choose **Assessments**.
3. Choose the name of the assessment that you want to generate an assessment report for.
4. Choose the **Assessment report selection** tab, and then choose **Generate assessment report**.

> **Tip**
>
> If **Generate assessment report** is greyed out, this means that no evidence was added to the assessment report yet.

5. In the pop-up window, provide a name and description for the assessment report, and review the assessment report details.
6. Choose **Generate assessment report** and wait a few minutes while your assessment report is generated.
7. Find and download your assessment report from the **Download center** page of the Audit Manager console.
   - Alternatively, you can go to your assessment report destination S3 bucket and download the assessment report from there.

Next steps

After you generate an assessment report, you can learn more about the following:

- **Find and download your assessment report** – Learn how to download your assessment report from the download center or from Amazon S3.
- **Explore your assessment report** – Learn how to navigate an assessment report and explore its contents.
- **Validate your assessment report** – Learn how to use the ValidateAssessmentReportIntegrity API operation to validate your assessment report.
- **Delete an unwanted assessment report** – Learn how to delete an unwanted report from the download center or from Amazon S3.
- **Generate assessment reports from evidence finder** – Learn how to generate assessment reports from your evidence finder search results.

Additional resources

To find answers to common questions and issues, see Troubleshooting assessment report issues in the *Troubleshooting* section of this guide.

Changing the status of an assessment control in AWS Audit Manager

You can change the status of an assessment control within your active assessment. Updating a control's status enables you to track its progress and indicate when you have reviewed it, keeping your assessment organized and up-to-date.

Prerequisites

The following procedure assumes that you have previously created an assessment, and its current status is active.

Make sure your IAM identity has appropriate permissions to manage an assessment in AWS Audit Manager. Two suggested policies that grant these permissions are AWSAuditManagerAdministratorAccess and Allow users management access to AWS Audit Manager.

Procedure

You can update an assessment control status using the Audit Manager console, the Audit Manager API, or the AWS Command Line Interface (AWS CLI).

> **Note**
>
> Changing a control status to *Reviewed* is final. After you set the status of a control to *Reviewed*, you can no longer change the status of that control or revert to a previous status.

Audit Manager console

To change an assessment control status on the Audit Manager console

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.

2. In the navigation pane, choose **Assessments**.
3. Choose the name of the assessment to open it.
4. From the assessment page, choose the **Controls** tab, scroll down to the **Control sets** table, and then choose the name of a control to open it.
5. Choose **Update control status** at the top right of the page, and then choose a status:

Status	Description
Under review	Choose this status if you haven't reviewed the control yet.
Reviewed	Choose this status if you have finished reviewing the evidence for this control, and you want to continue collectin g or adding evidence.
Inactive	Choose this status if you want to stop collecting automated evidence for this control.

6. Choose **Update control status** to confirm your choice.

AWS CLI

To change an assessment control status in the AWS CLI

1. Run the list-assessments command.

```
aws auditmanager list-assessments
```

The response returns a list of assessments. Find the assessment that contains the control that you want to update, and take note of the assessment ID.

2. Run the get-assessment command and specify the assessment ID from step 1.

In the following example, replace the *placeholder text* with your own information.

```
 aws auditmanager get-assessment --assessment-
id 1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4e5f6g
```

In the response, find the control that you want to update and take note of the control ID and its control set ID.

3. Run the update-assessment-control command and specify the following parameters:

   - `--assessment-id` – The assessment that the control belongs to.
   - `--control-set-id` – The control set that the control belongs to.
   - `--control-id` – The control that you want to update.
   - `--control-status` – Set this value to `UNDER_REVIEW`, `REVIEWED`, or `INACTIVE`.

   In the following example, replace the *placeholder text* with your own information.

   ```
   aws auditmanager update-assessment-control --assessment-
   id 1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4e5f6g --control-set-id "My control set" --
   control-id 2b3c4d5e-2b3c-2b3c-2b3c-2b3c4d5f6g7h --control-status REVIEWED
   ```

Audit Manager API

To change an assessment control status using the API

1. Use the ListAssessments operation.

   In the response, find the assessment that contains the control that you want to update, and take note of the assessment ID.

2. Use the GetAssessment operation and specify the assessment ID from step 1.

   In the response, find the control that you want to update and take note of the control ID and its control set ID.

3. Use the UpdateAssessmentControl operation and specify the following parameters:

   - `assessmentId` – The assessment that the control belongs to.
   - `controlSetId` – The control set that the control belongs to.
   - `controlId` –The control that you want to update.
   - `controlStatus` – Set this value to `UNDER_REVIEW`, `REVIEWED`, or `INACTIVE`.

For more information about these API operations, choose any of the links in the previous procedure to read more in the *AWS Audit Manager API Reference*. This includes information about how to use these operations and parameters in one of the language-specific AWS SDKs.

Next steps

When you're ready to change the status of the assessment, see Changing the status of an assessment to inactive in AWS Audit Manager.

Changing the status of an assessment to inactive in AWS Audit Manager

When you no longer need to collect evidence for an assessment, you can change the assessment status to *Inactive*. When the status of an assessment changes to inactive, the assessment stops collecting evidence. As a result, you no longer incur any charges for that assessment.

In addition to stopping evidence collection, Audit Manager makes the following changes to the controls that are within the inactive assessment:

- All control sets change to *Reviewed* status.
- All controls that are *Under review* change to *Reviewed* status.
- Delegates for the inactive assessment can no longer view or edit its controls and control sets.

Prerequisites

The following procedure assumes that you have previously created an assessment, and its current status is active.

Make sure your IAM identity has appropriate permissions to manage an assessment in AWS Audit Manager. Two suggested policies that grant these permissions are AWSAuditManagerAdministratorAccess and Allow users management access to AWS Audit Manager.

Procedure

You can update an assessment status using the Audit Manager console, the Audit Manager API, or the AWS Command Line Interface (AWS CLI).

Warning

This action is irreversible. We recommend that you proceed with caution and make sure that you want to mark your assessment as inactive. When an assessment is inactive, you have read-only access to its contents. This means that you can still review previously collected evidence and generate assessment reports. However, you can't edit the inactive assessment, add comments, or upload any manual evidence.

Audit Manager console

To change an assessment status to inactive on the Audit Manager console

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the navigation pane, choose **Assessments**.
3. Choose the name of the assessment to open it.
4. On the upper-right corner of the page, choose **Update assessment status**, and then choose **Inactive**.
5. Choose **Update status** in the pop-up window to confirm that you want to change the status to inactive.

The changes to the assessment and its controls take effect after approximately one minute.

AWS CLI

To change an assessment status to inactive in the AWS CLI

1. First, identify the assessment that you want to update. To do this, run the list-assessments command.

```
aws auditmanager list-assessments
```

   The response returns a list of assessments. Find the assessment that you want to deactivate, and take note of the assessment ID.

2. Next, run the update-assessment-status command and specify the following parameters:

- `--assessment-id` – Use this parameter to specify the assessment that you want to deactivate.
- `--status` – Set this value to `INACTIVE`.

In the following example, replace the *`placeholder text`* with your own information.

```
aws auditmanager update-assessment-status --assessment-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 --status INACTIVE
```

The changes to the assessment and its controls take effect after approximately one minute.

Audit Manager API

To change an assessment status to inactive using the API

1. Use the ListAssessments operation to find the assessment that you want to deactivate, and take note of the assessment ID.
2. Use the UpdateAssessmentStatus operation and specify the following parameters:
   - assessmentId – Use this parameter to specify the assessment that you want to deactivate.
   - status – Set this value to `INACTIVE`.

The changes to the assessment and its controls take effect after approximately one minute.

For more information about these API operations, choose any of the links in the previous procedure to read more in the *AWS Audit Manager API Reference*. This includes information about how to use these operations and parameters in one of the language-specific AWS SDKs.

Next steps

When you're certain that you no longer need your inactive assessment, you can clean up your Audit Manager environment by deleting the assessment. For instructions, see Deleting an assessment in AWS Audit Manager.

Deleting an assessment in AWS Audit Manager

When you no longer need an assessment, you can delete it from your Audit Manager environment. This enables you to clean up your workspace and focus on the assessments that are relevant to your current tasks and priorities.

> **Tip**
>
> If your goal is to reduce costs, consider changing the assessment status to inactive instead of deleting it. This action stops evidence collection, and places your assessment in a read-only state where you can review the evidence that was previously collected. Inactive assessments don't incur any charges.

Prerequisites

The following procedure assumes that you have previously created an assessment.

Make sure your IAM identity has appropriate permissions to delete an assessment in AWS Audit Manager. Two suggested policies that grant these permissions are AWSAuditManagerAdministratorAccess and Allow users management access to AWS Audit Manager.

Procedure

You can delete assessments using the Audit Manager console, the Audit Manager API or the AWS Command Line Interface (AWS CLI).

> **Warning**
>
> This action permanently deletes your assessment and all of the evidence that it collected. You cannot recover this data. As a result, we recommend that you proceed with caution and make sure that you want to delete your assessment.

Audit Manager console

To delete an assessment on the Audit Manager console

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the navigation pane, choose **Assessments**.
3. Select the assessment that you want to delete, and choose **Delete**.

AWS CLI

To delete an assessment in the AWS CLI

1. First, identify the assessment that you want to delete. To do this, run the list-assessments command.

   ```
   aws auditmanager list-assessments
   ```

   The response returns a list of assessments. Find the assessment that you want to delete, and take note of the assessment ID.
2. Next, use the delete-assessment command and specify the `--assessment-id` of the assessment that you want to delete.

   In the following example, replace the *placeholder text* with your own information.

   ```
   aws auditmanager delete-assessment --assessment-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

Audit Manager API

To delete an assessment using the API

1. Use the ListAssessments operation to find the assessment that you want to delete.

   In the response, take note of the assessment ID.
2. Use the DeleteAssessment operation and specify the assessmentId of the assessment that you want to delete.

For more information about these API operations, choose any of the previous links to read more in the *AWS Audit Manager API Reference*. This includes information about how to use these operations and parameters in one of the language-specific AWS SDKs.

Additional resources

For information about data retention in Audit Manager, see Deletion of Audit Manager data.

Delegations in AWS Audit Manager

As you navigate through the assessment process in AWS Audit Manager, you might encounter situations where you need help from subject matter experts to review and validate the collected evidence. This is where the concept of delegations comes into play.

Key points

Delegations enable audit owners to assign specific control sets to delegates – individuals with specialized expertise in relevant areas. By using the delegation feature, you can ensure that the evidence for each control is thoroughly evaluated by the appropriate personnel. This helps you to streamline the review process and enhance the overall accuracy and reliability of your assessments. Whether you need guidance on interpreting technical evidence, clarifying compliance requirements, or gaining deeper insights into specific domains, delegations enable you to collaborate effectively with subject matter experts.

At a high level, the delegation process is as follows:

1. The audit owner chooses a control set in their assessment and delegates it for review.
2. The delegate reviews those controls and their evidence, and submits the control set back to the audit owner when finished.
3. The audit owner is notified that the review is complete, and checks the reviewed controls for any remarks from the delegate.

> **Note**
>
> An AWS account can be an audit owner or a delegate in different AWS Regions.

Additional resources

Use the following sections of this chapter to learn more about how to manage delegation tasks in AWS Audit Manager.

- Understanding the different delegation tasks for audit owners

Understanding the different delegation tasks for audit owners

As an audit owner in AWS Audit Manager, you're responsible for managing assessments and ensuring compliance within your organization. While you have expertise in governance, risk, and compliance, there might be times when you have questions or need assistance from subject matter experts to review and interpret specific technical evidence or controls. This is where the delegation feature in Audit Manager becomes useful.

Key points

Creating a delegation enables you to assign control sets within an assessment to other Audit Manager users (known as delegates) who have specialized knowledge or technical expertise in relevant areas. These delegates can then review the assigned control sets, analyze the collected evidence, provide comments or additional evidence if needed, and update the status of individual controls.

The delegation process streamlines the review and validation of controls by leveraging the collective expertise within your organization. It ensures that each control is thoroughly evaluated by the most qualified personnel, enhancing the accuracy and reliability of your assessments.

Additional resources

The following sections guide you through the different tasks that are associated with managing delegations as an audit owner. This includes how to delegate control sets, track the status of

delegations, and manage completed delegations. By effectively using delegations, you can collaborate with subject matter experts, leverage their specialized knowledge, and maintain a comprehensive and well-informed audit process within Audit Manager.

- Delegating a control set for review in AWS Audit Manager
- Finding and reviewing the delegations that you've sent in AWS Audit Manager
- Deleting your completed delegations in AWS Audit Manager

Delegating a control set for review in AWS Audit Manager

When you need assistance from a subject matter expert, you can choose the AWS account that you want to help you, and then delegate a control set to them for review.

Delegate permissions

The below policy is attached to a delegate to whom the control set is delegated to.

Audit Manager replaces the *placeholder text* with your account and resource identifiers before attaching the policy.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Delegate",
            "Effect": "Allow",
            "Principal": {
                "AWS": "Principal for user/role who is delegated a Control Set of
 the Assessment"
            },
            "Action": [
                "auditmanager:UpdateAssessmentControl",
                "auditmanager:UpdateAssessmentControlSetStatus",
                "auditmanager:GetEvidenceFoldersByAssessmentControl",
                "auditmanager:BatchImportEvidenceToAssessmentControl",
                "auditmanager:GetEvidenceFolder",
```

```
                "auditmanager:GetEvidence",
                "auditmanager:GetEvidenceByEvidenceFolder"
            ],
            "Resource": "arn:aws:auditmanager:us-
east-1:123456789012:assessment/assessment_ID/controlSet/control_set_ID"
        }
    ]
}
```

Prerequisites

Make sure your IAM identity has appropriate permissions to create a delegation in AWS Audit Manager. Two suggested policies that grant these permissions are Allow users full administrator access to AWS Audit Manager and Allow users management access to AWS Audit Manager.

Procedure

You can use either of the following procedures to delegate a control set.

Delegating a control set from an assessment page

To delegate a control set from the assessment page

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the navigation pane, choose **Assessments**.
3. Select the name of the assessment that contains the control set that you want to delegate.
4. From the assessment page, choose the **Controls** tab. This displays the control status summary and the list of controls in the assessment.
5. Select a control set and choose **Delegate control set**.
6. Under **Delegate selection**, a list of users and roles is displayed. Choose a user or role, or use the search bar to look for one.
7. Under **Delegation details**, review the control set name and the assessment name.
8. (Optional) Under **Comments**, add a comment with instructions to help the delegate fulfill their review task. Don't include any sensitive information in your comment.
9. Choose **Delegate control set**.

10. A green success banner confirms the successful delegation of the control set. Choose **View delegation** to see the delegation request. You can also view your delegations at any time by choosing **Delegations** in the left navigation pane of the AWS Audit Manager console.

Delegating a control set from the delegations page

To delegate a control set from the delegations page

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the navigation pane, choose **Delegations**.
3. From the delegations page, choose **Create delegation**.
4. Under **Choose assessment and control set**, specify the assessment and the control set that you want to delegate.
5. Under **Delegate selection**, you will see a list of users and roles. Choose a user or role, or use the search bar to look for one.
6. (Optional) Under **Comments**, add a comment with instructions to help the delegate fulfill their review task. Don't include any sensitive information in your comment.
7. Choose **Create delegation**.
8. A green success banner confirms the successful delegation of the control set. Choose **View delegation** to see the delegation request. You can also view your delegations at any time by choosing **Delegations** in the left navigation pane of the AWS Audit Manager console.

After you delegate a control set for review, the delegate receives a notification and can then begin to review the control set. This process that delegates follow is described in Understanding the different delegation tasks for delegates.

Next steps

To revisit your delegation at a later date, see Finding and reviewing the delegations that you've sent in AWS Audit Manager.

Finding and reviewing the delegations that you've sent in AWS Audit Manager

You can access a list of your delegations at any time by choosing **Delegations** in the left navigation pane of Audit Manager. The delegations page contains a list of your active and completed delegations.

When a delegation is completed, you receive a notification in Audit Manager. You might also receive comments with remarks from the delegate. The following procedure explains how to check your delegations in Audit Manager after they are completed, and how to view any comments that the delegate might have left for you.

Prerequisites

Make sure your IAM identity has appropriate permissions to view a delegation in AWS Audit Manager. Two suggested policies that grant these permissions are Allow users full administrator access to AWS Audit Manager and Allow users management access to AWS Audit Manager.

Procedure

Follow these steps to find and review the delegations that you previously created.

To view a completed delegation and check for comments

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the navigation pane, choose **Delegations**.
3. Review the **Delegations** page, which includes a table with the following information:

Name	Description
Delegated to	The AWS account that you delegated the control set to.
Date	The date when you delegated the control set.
Status	The current status of the delegation.
Assessment	The name of the assessment with a link to the assessment detail page.
Control set	The name of the control set that was delegated for review.

4. Find the assessment and control set that the delegate reviewed and submitted to you, and choose the name of the assessment to open it.
5. Under the **Controls** tab of the assessment detail page, scroll down to the **Control sets** table.
6. Under **Controls grouped by control set**, find the name of the control set that you delegated.
7. Expand the name of the control set to show its controls, and choose the name of a control to open the control detail page.
8. Choose the **Comments** tab to view any remarks added by the delegate for that particular control.
9. When you're satisfied that the review is complete for a control set, select the control set and choose **Complete control set review**.

> **Important**
>
> Audit Manager collects evidence continuously. As a result, additional new evidence might be collected *after* the delegate completes their review of a control.
> If you only want to use reviewed evidence in your assessment reports, you can refer to the *control reviewed* timestamp to determine when evidence was reviewed. This timestamp can be found on the Changelog tab of the control detail page. You can then use this timestamp to identify which evidence you add to your assessment reports.

Next steps

To delete a delegation after it's complete and you no longer need it, see Deleting your completed delegations in AWS Audit Manager.

Deleting your completed delegations in AWS Audit Manager

There may be circumstances where you create a delegation but later no longer need assistance reviewing that control set. When this happens, you can delete an active delegation in Audit Manager. You can also delete completed delegations that you no longer want to see on the delegations page.

Prerequisites

Make sure your IAM identity has appropriate permissions to delete a delegation in AWS Audit Manager. Two suggested policies that grant these permissions are Allow users full administrator access to AWS Audit Manager and Allow users management access to AWS Audit Manager.

Procedure

To delete a delegation

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the navigation pane, choose **Delegations**.
3. On the **Delegations** page, select the delegation that you want to cancel and then choose **Remove delegation**.
4. In the pop-up window that appears, choose **Delete** to confirm your choice.

Understanding the different delegation tasks for delegates

As a delegate in AWS Audit Manager, you play an important role in supporting audit owners during the assessment process. While audit owners are responsible for managing assessments and ensuring overall compliance, they might sometimes need assistance from subject matter experts with reviewing and interpreting specific technical evidence that falls outside their areas of expertise. In such scenarios, your knowledge and skills become invaluable.

Key points

The delegation feature enables audit owners to assign specific control sets to you for review, tapping into your specialized business or technical expertise. This collaborative approach not only enhances the accuracy and reliability of assessments but also streamlines the review process, enabling audit owners to focus on their core responsibilities while you concentrate your efforts on the areas where your expertise is most valuable.

As a delegate, you might receive requests from audit owners to review evidence associated with assigned control sets. You can help audit owners by reviewing control sets and their related evidence, adding comments, uploading additional evidence, and updating the status of each control that you review.

> **Note**
>
> Audit owners delegate specific control sets for review, not entire assessments. As a result, delegates have limited access to assessments. Delegates can review evidence, add comments, upload manual evidence, and update the control status for each of the controls in the control set. For more information about roles and permissions in Audit Manager, see Recommended policies for user personas in AWS Audit Manager.

Additional resources

In the following sections, you can learn more about the tasks that are associated with managing delegations as a delegate. This includes how to view incoming delegation requests, review assigned control sets, provide comments and additional evidence, and submit your reviewed controls back to the audit owner.

- Viewing your notifications for incoming delegation requests
- Reviewing the delegated control set and its related evidence
- Adding comments about a control during a control set review
- Marking a control as reviewed in AWS Audit Manager
- Submitting a reviewed control set back to the audit owner

Viewing your notifications for incoming delegation requests

When an audit owner requests your assistance with reviewing a control set, you receive a notification that informs you of the control set that they delegated to you.

Prerequisites

Make sure your IAM identity has appropriate permissions to view notifications in AWS Audit Manager. Two suggested policies that grant these permissions are Allow users full administrator access to AWS Audit Manager and Allow users management access to AWS Audit Manager.

Procedure

To view your notifications

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. Choose **Notifications** in the left navigation pane.
3. On the **Notifications** page, review the list of control sets that have been delegated to you for review. The table includes the following information:

Name	Description
Date	The date when the control set was delegated.
Assessment	The name of the assessment that's associated with the control set.
Control set	The name of the control set.
Source	The user or role that delegated the control set to you.
Description	Instructions that are provided by the audit owner.

> **Tip**
>
> You can also subscribe to an SNS topic to receive email alerts when a control set is delegated to you for review. For more information, see Notifications in AWS Audit Manager.

Next steps

When you're ready to start reviewing the controls that were delegated to you, see Reviewing the delegated control set and its related evidence.

Reviewing the delegated control set and its related evidence

You can assist audit owners by reviewing the control sets that they have delegated to you.

You can examine these controls and their related evidence to determine if any additional action is needed. Such additional action could include manually uploading additional evidence to demonstrate compliance, or leaving a comment that details the remediation steps that you followed.

Prerequisites

Make sure your IAM identity has appropriate permissions to view a control set in AWS Audit Manager. Two suggested policies that grant these permissions are Allow users full administrator access to AWS Audit Manager and Allow users management access to AWS Audit Manager.

Procedure

To review a control set

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the navigation pane, choose **Notifications**.
3. On the **Notifications** page, you can see a list of control sets that were delegated to you. Identify which control set you want to review, and choose the name of the related assessment to open the assessment detail page.
4. Under the **Controls** tab of the assessment detail page, scroll down to the **Control sets** table.
5. Under the **Controls grouped by control set** column, expand the name of a control set to show its controls.
6. Choose the name of a control to open the control detail page.
7. (Optional) Choose **Update control status** to change the status of the control. While your review is in progress, you can mark the status as **Under Review**.
8. Review information about the control in the **Evidence folders**, **Details**, **Data sources**, **Comments**, and **Changelog** tabs.

   - To learn about each of these tabs and how to understand the data that they contain, see Reviewing an assessment control in AWS Audit Manager.

To review the evidence for a control

1. From the control detail page, choose the **Evidence folders** tab.

2. Navigate to the **Evidence folders** table to see a list of folders that contain evidence for that control. These folders are organized and named based on the date when the evidence was collected.
3. Choose the name of an evidence folder to open it. Then, review a summary of all evidence gathered on that date.
   - This summary includes the total number of compliance check issues that were reported directly from AWS Security Hub, AWS Config, or both.
   - To learn more about this information, see Reviewing an evidence folder in AWS Audit Manager.
4. From the evidence folder summary page, navigate to the **Evidence** table. Under the **Time** column, choose a piece of evidence to open.
5. Review the details of the evidence.
   - To learn more about this information, see Reviewing evidence in AWS Audit Manager.

Next steps

In some cases you might need to provide additional evidence to demonstrate compliance. In these cases, you can manually upload evidence. For instructions, see Adding manual evidence in AWS Audit Manager.

If you want to leave comments about one or more of the controls that were delegated to you, see Adding comments about a control during a control set review.

Adding comments about a control during a control set review

You can add comments for any controls that you review. These comments are visible to the audit owner.

Prerequisites

Make sure your IAM identity has appropriate permissions to add comments to an assessment control in AWS Audit Manager. Two suggested policies that grant these permissions are Allow users full administrator access to AWS Audit Manager and Allow users management access to AWS Audit Manager.

Procedure

To add a comment to a control

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. Choose **Notifications** in the left navigation pane.
3. On the **Notifications** page, review the list of control sets that were delegated to you.
4. Find the control set that contains the control that you want to leave a comment for, then choose the name of the related assessment to open the assessment.
5. Choose the **Controls** tab, scroll down to the **Control sets** table, and then select the name of a control to open it.
6. Choose the **Comments** tab.
7. Under **Send comments**, enter your comment in the text box.
8. Choose **Submit comment** to add your comment. Your comment then appears under the **Previous comments** section of the page, along with any other comments regarding this control.

Next steps

When you've finished reviewing the control, follow the steps in Marking a control as reviewed in AWS Audit Manager.

Marking a control as reviewed in AWS Audit Manager

You can indicate your review progress by updating the status of individual controls within a control set.

Changing the control status is optional. However, we recommend that you change the status of each control to **Reviewed** as you complete your review for that control. Regardless of the status of each individual control, you can still submit the controls back to the audit owner.

Prerequisites

Make sure your IAM identity has appropriate permissions to update an assessment control status in AWS Audit Manager. Two suggested policies that grant these permissions are Allow users full

administrator access to AWS Audit Manager and Allow users management access to AWS Audit Manager.

Procedure

To mark a control as reviewed

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. Choose **Notifications** in the left navigation pane.
3. On the **Notifications** page, review the list of control sets that were delegated to you.
4. Find the control set that you want to mark as reviewed, then choose the name of the related assessment to open the assessment.
5. Under the **Controls** tab of the assessment detail page, scroll down to the **Control sets** table.
6. Under the **Controls grouped by control set** column, expand the name of a control set to show its controls.
7. Choose the name of a control to open the control detail page.
8. Choose **Update control status** and change the status to **Reviewed**.
9. In the pop-up window that appears, choose **Update control status** to confirm that you finished reviewing the control.

Next steps

To complete the delegation process, see Submitting a reviewed control set back to the audit owner.

Submitting a reviewed control set back to the audit owner

After reviewing the control set, adding comments or additional evidence, and updating the status of individual controls, you reach an important step – submitting the reviewed control set back to the audit owner. Submitting the reviewed control set marks the completion of your delegated tasks, and enables the audit owner to incorporate your insights and recommendations into the overall assessment.

Prerequisites

Make sure your IAM identity has appropriate permissions to submit the reviewed control set back to the audit owner in AWS Audit Manager. Two suggested policies that grant these permissions are

Allow users full administrator access to AWS Audit Manager and Allow users management access to AWS Audit Manager.

Procedure

Follow these steps to submit the control set to the audit owner.

To submit a reviewed control set back to the audit owner

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. Choose **Notifications** in the left navigation pane.
3. Review the list of control sets that were delegated to you. Find the control set that you want to submit back to the audit owner, and choose the name of the related assessment.
4. Scroll down to the **Control sets** table, select the control set that you want to submit to the audit owner, and then choose **Submit for review**.
5. In the pop-up window that appears, you can add comments before choosing **Submit for review**.

Assessment reports

An *assessment report* summarizes the selected evidence that was collected for an assessment. It also contains links to PDF files with details about each piece of evidence. The specific contents, organization, and naming convention of an assessment report depend on the parameters that you choose when you generate the report.

Assessment reports help you to select and compile the evidence that's relevant for your audit. However, they don't assess the compliance of the evidence itself. Instead, Audit Manager simply provides the selected evidence details as an output that you can share with your auditor.

Contents

Understanding the assessment report folder structure

When you download an assessment report, Audit Manager produces a zip folder. This contains your assessment report and related evidence files in nested subfolders.

The zip folder is structured as follows:

- **Assessment folder** (example: `myAssessmentName-a1b2c3d4`) – The root folder.
  - **Assessment report folder** (example: `reportName-a1b2c3d4e5f6g7`) – A subfolder where you can find the AssessmentReportSummary.pdf, digest.txt, and README.txt files.
    - **Evidence by control folder** (example: `controlName-a1b2c3d4e5f6g`) – A subfolder that groups evidence files by the related control.
      - **Evidence by data source folder** (example: `CloudTrail`, `Security Hub`) – A subfolder that groups evidence files by the data source type.
        - **Evidence by date folder** (example: `2022-07-01`) – A subfolder that groups evidence files by the evidence collection date.
          - **Evidence files** – The files that contain details about individual pieces of evidence.

Navigating an assessment report

Start by opening the zip folder and navigating one level down to the assessment report folder. Here, you can find the assessment report PDF and the README.txt file.

You can review the README.txt file to understand the structure and the contents of the zip folder. It also provides reference information about the naming conventions for each file. This information can help you navigate directly to a subfolder or evidence file if you're looking for a specific item.

Otherwise, to browse evidence and locate the information that you need, open the assessment report PDF. This gives you a high-level overview of the report, and a summary of the assessment that the report was created from.

Next, use the table of contents (TOC) to explore the report. You can choose any hyperlinked control in the TOC to jump directly to a summary of that control.

When you're ready to review evidence details for a control, you can do so by choosing the hyperlinked evidence name. For automated evidence, the hyperlink opens a new PDF file with details about that evidence. For manual evidence, the hyperlink takes you to the S3 bucket that contains the evidence.

> **Tip**
>
> The breadcrumb navigation at the top of each page shows your current location in the assessment report as you browse controls and evidence. Select the hyperlinked TOC to navigate back to the TOC at any time.

Reviewing the sections of an assessment report

Use the following information to learn more about each section of an assessment report.

> **Note**
>
> When you see a hyphen (-) next to any of the attributes in the following sections, this indicates that the value of that attribute is null, or a value doesn't exist.

Cover page

The cover page includes the name of the assessment report. It also displays the date and time that the report was generated, along with the account ID of the user who generated the report.

The cover page is formatted as follows. Audit Manager replaces the *placeholders* with the information that's relevant to your report.

```
Assessment report name
Report generated on MM/DD/YYYY at HH:MM:SS AM/PM UCT by AccountID
```

Overview page

The overview page has two parts: a summary of the report itself, and a summary of the assessment that's being reported on.

Report summary

This section summarizes the assessment report.

Name	Description
Report name	The name of the report.
Description	The description that's entered by the audit owner when they generate the report.
Date generated	The date when the report was generated. The time is represented in Coordinated Universal Time (UTC).
Total controls included	The number of controls that are included in the report and have collected evidence. This is a subset of the total number of controls in the assessment.
AWS accounts included	The number of AWS accounts that are included in the report and have collected evidence. This is a subset of the total number of AWS accounts in the assessment.
Assessment report selection	The number of evidence items that are selected for inclusion in the report. This includes the total number of compliance check issues that are found in the report.

Assessment summary

This section summarizes the assessment that the report relates to.

Name	Description
Assessment name	The name of the assessment that the report was generated from.

Name	Description
Status	The status of the assessment at the time when the report was generated.
Assessnent Region	The AWS Region that the assessment was created in.
AWS accounts in scope	The list of AWS accounts that are in the scope of the assessment.
Framework name	The name of the framework that the assessment was created from.
Audit owners	The user or role of the assessment's audit owners.
Last updated	The date when the assessment was last updated. The time is represented in UTC.

Table of contents page

The TOC displays the full contents of the assessment report. The contents are grouped and organized based on the control sets that are included in the assessment. Controls are listed underneath their respective control set.

Choose any item in the table of contents to navigate directly to that section of the report. You can either choose a control set or go directly to a control.

Control page

The control page has two parts: a summary of the control itself, and a summary of the evidence that was collected for the control.

Control summary

This section includes the following information.

Name	Description
Control name	The name of the control.

Name	Description
Description	The description of the control.
Control set	The name of the control set that the control belongs to.
Testing information	The recommended testing procedures for this control.
Action plan	The recommended actions to perform if the control isn't fulfilled.
Assessment report selection	The number of evidence items related to this control that were included in the assessment report. This includes the number of compliance check issues that were found for this control's evidence.

Collected evidence

This section shows the evidence that was collected for the control. The evidence is grouped by folders, which are organized and named by the evidence collection date. Next to each evidence folder name is the total number of compliance check issues for that folder.

Underneath each evidence folder name is a list of hyperlinked evidence names.

- Automated evidence names start with an evidence collection timestamp, followed by the service code, event name (up to 20 characters), account ID, and a unique 12-character unique ID.

  For example: `21-30-24_IAM_CreateUser_111122223333_a1b2c3d4e5f6`

  For automated evidence, the hyperlinked name opens a new PDF file with a summary and further details.
- Manual evidence names start with an evidence upload timestamp, followed by the `manual` label, account ID, and a 12-character unique ID. They also include the first 10 characters of the file name, and the file extension (up to 10 characters).

  For example: `00-00-00_manual_111122223333_a1b2c3d4e5f6_myimage.png`

  For manual evidence, the hyperlinked name takes you to the S3 bucket that contains that evidence.

Next to each evidence name is the result of the compliance check for that item.

- For automated evidence that's collected from AWS Security Hub or AWS Config, a **Compliant**, **Non-compliant**, or **Inconclusive** result is reported.
- For automated evidence that's collected from AWS CloudTrail and API calls, and for all manual evidence, an **Inconclusive** result is shown.

Evidence summary page

The evidence summary page includes the following information.

Name	Description
ID	The unique identifier for the evidence.
Date collected	The date when the evidence was created or uploaded.
Description	A description of the evidence, including the account ID and the data source type.
Assessment name	The name of the assessment that the report was generated from.
Framework name	The name of the framework that the assessment was created from.
Control name	The name of the control that the evidence supports.
Control set name	The name of the control set that the related control belongs to.
Control description	The description of the control that the evidence supports.
Testing information	The recommended testing procedures for the control.
Action plan	The recommended actions to perform if the control is not fulfilled .
AWS Region	The name of the Region that's associated with the evidence.
IAM ID	The ARN of the user or role that's associated with the evidence.

Name	Description
AWS account	The AWS account ID that's associated with the evidence.
AWS service	The name of the AWS service that's associated with the evidence.
Event name	The name of the evidence event.
Event time	The time when the evidence event occurred.
Data source	Where the evidence was collected or uploaded from. The data source type can be either AWS Config, Security Hub, AWS API calls, CloudTrail, or Manual.
Evidence by type	The category of the evidence • *Compliance check* evidence is collected from AWS Config or Security Hub. • *User activity* evidence is collected from CloudTrail logs. • *Configuration data* evidence is collected from snapshots of other AWS services. • *Manual* evidence is evidence that you upload manually.
Compliance check status	The evaluation status for evidence that falls under the *compliance check* category. • For automated evidence that's collected from AWS Security Hub or AWS Config, a **Compliant**, **Non-compliant**, or **Inconclusive** result is reported. • For automated evidence that's collected from AWS CloudTrail and API calls, and for all manual evidence, an **Inconclusive** result is shown.

Evidence detail page

The evidence detail page shows the name of the evidence and an evidence detail table. This table provides a detailed breakdown of each element of the evidence so that you can understand the

data and validate that it's correct. Depending on the data source of the evidence, the contents of the evidence detail page vary.

> **Tip**
>
> The breadcrumb navigation at the top of each page shows your current location as you browse evidence details. Select **Evidence summary** to navigate back to the evidence summary at any time.

Validating an assessment report

When you generate an assessment report, Audit Manager produces a report file checksum called `digest.txt`. You can use this file to validate the integrity of the report and ensure that no evidence was modified after the report was created. It contains a JSON object with signatures and hashes that are invalidated if any part of the report archive is altered.

To validate the integrity of an assessment report, use the ValidateAssessmentReportIntegrity API that's provided by Audit Manager.

Additional resources

To find answers to common questions and issues, see Troubleshooting assessment report issues in the *Troubleshooting* section of this guide.

Evidence finder

Evidence finder provides a powerful way to search for evidence in Audit Manager. Instead of browsing deeply nested evidence folders to find what you're looking for, you can now use evidence finder to quickly query your evidence. If you use evidence finder as a delegated administrator, you can search for evidence across all member accounts in your organization.

Using a combination of filters and groupings, you can progressively narrow the scope of your search query. For example, if you want a high-level view of your system health, perform a broad search and filter by assessment, date range, and resource compliance. If your goal is to remediate a specific resource, you can perform a narrow search to target evidence for a specific control or resource ID. After you define your filters, you can group and then preview the matching search results before creating an assessment report.

To use evidence finder, you must enable this feature from your Audit Manager settings.

Key points

Understanding how evidence finder works with CloudTrail Lake

Evidence finder uses AWS CloudTrail Lake querying and storage capability. Before you start using evidence finder, it's helpful to understand a little more about how CloudTrail Lake works.

CloudTrail Lake aggregates data into a single, searchable event data store that supports powerful SQL queries. This means that you can search for data across your organization and within custom time ranges. With evidence finder, you can use this search functionality directly in the Audit Manager console.

When you request to enable evidence finder, Audit Manager creates an event data store on your behalf. After evidence finder is enabled, all of your future Audit Manager evidence is ingested into the event data store where it's available for evidence finder search queries. After you enable evidence finder, we also backfill the newly created event data store with your past two years' worth of evidence data. If you enable evidence finder as a delegated administrator, we backfill the data for all member accounts in your organization.

All of your evidence data, whether backfilled or new, is retained in the event data store for 2 years. You can change the default retention period at any time. For instructions, see Update an event data

store in the *AWS CloudTrail User Guide*. You can keep data in an event data store for up to 7 years, or 2,555 days.

> **Note**
>
> When new evidence data is added to the event data store, CloudTrail Lake charges are incurred for data storage and ingestion.
> For CloudTrail Lake queries, you pay as you go. This means that for each search query that you run in evidence finder, you're charged for the data that's scanned.
> For more information about CloudTrail Lake pricing, see AWS CloudTrail pricing.

Next steps

To get started, enable evidence finder from your Audit Manager settings. For instructions, see Enabling evidence finder.

Additional resources

- Searching for evidence in evidence finder
- Viewing results in evidence finder
- Filter and grouping options for evidence finder
- Example use cases for evidence finder
- Troubleshooting evidence finder issues

Searching for evidence in evidence finder

You can use evidence finder to perform targeted searches and quickly surface relevant evidence for review.

On this page, you'll learn how to filter your searches by criteria like assessment, date range, resource compliance status, and additional attributes. Applying these filters narrows your search scope to just the evidence you need. You can also group your results by certain fields to better analyze patterns.

Prerequisites

Make sure that you completed the steps to enable evidence finder in your Audit Manager settings. For instructions, see Enabling evidence finder.

In addition, make sure that you have permissions to perform search queries in evidence finder. For an example permission policy that you can use, see Allow users to run search queries in evidence finder.

Procedure

Follow these steps to search for evidence in the Audit Manager console.

1. Perform a search query
2. Stop an in-progress search query (optional)
3. Edit the filters for your search query (optional)

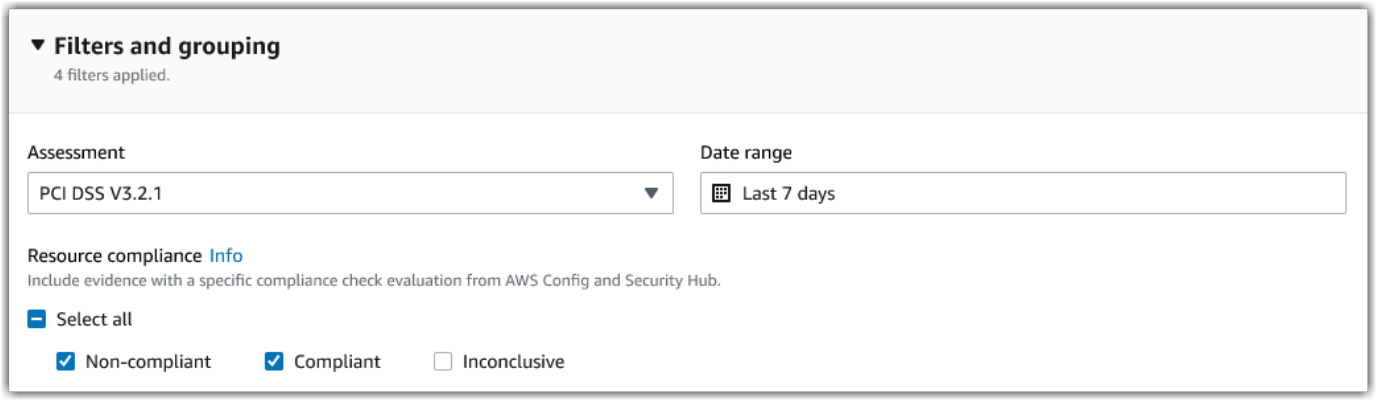
> **Note**
>
> You can also use the CloudTrail API to query your evidence data. For more information, see StartQuery in the *AWS CloudTrail API Reference*. If you prefer to use the AWS CLI, see Start a query in the *AWS CloudTrail User Guide*.

Performing a search query

Follow these steps to perform a search query in evidence finder.

To search for evidence

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the navigation pane, choose **Evidence finder**.
3. Next, apply filters to narrow the scope of your search.
    a. For **Assessment**, choose an assessment.
    b. For **Date range**, select a range.
    c. For **Resource compliance**, select an evaluation status.

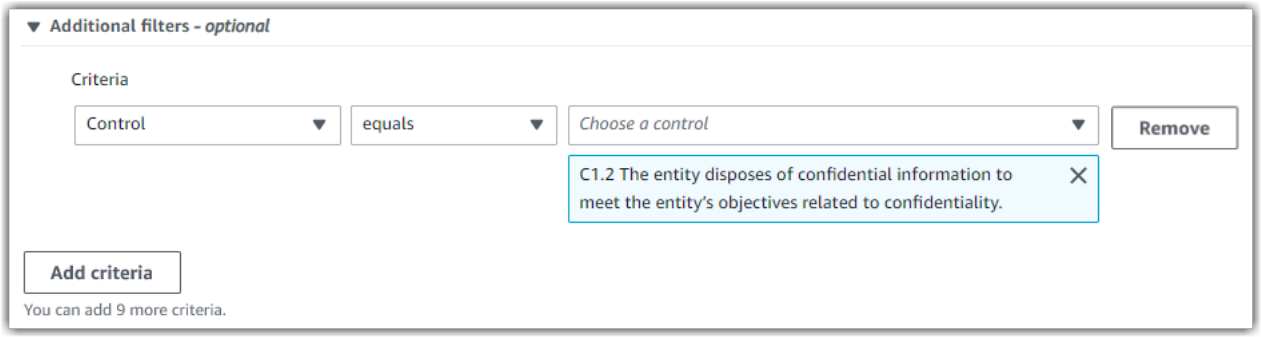


4. (Optional) Choose **Additional filters - optional** to narrow the search even further.

   a. Choose **Add criteria**, select a criteria, and then select one or more values for that criteria.

   b. Continue to build more filters in the same way.

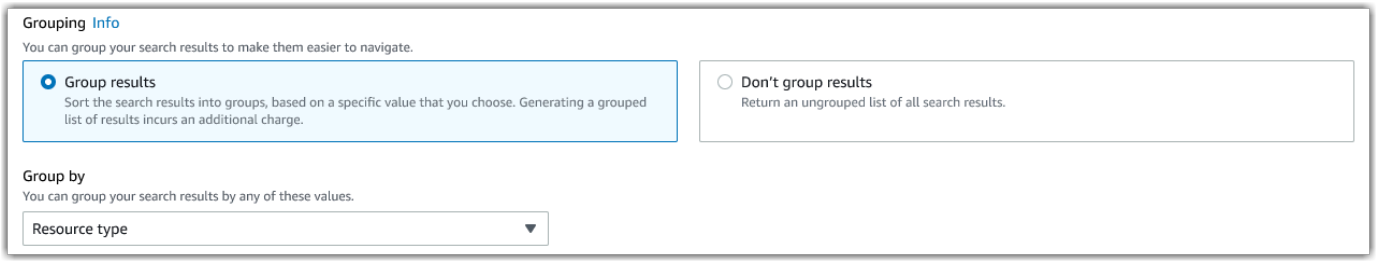
   c. To remove an unwanted filter, choose **Remove**.



5. Under **Grouping**, specify whether you want to group the search results.

   a. If you want to group the results, select a value to group the results by.

   b. If you don't want to group the results, proceed to step 6.



6. Choose **Search**.

Your search might take a few minutes, depending on the amount of evidence data that you have. Feel free to navigate away from evidence finder while the search is in progress. A flash bar notifies you when the search results are ready.

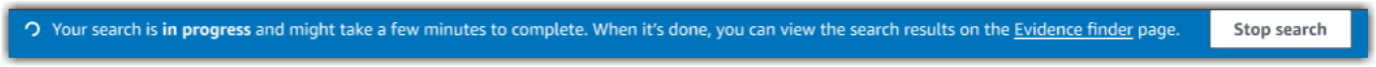
Stopping a search query

If you want to stop a search query for any reason, follow these steps.

> **Note**
>
> Stopping a search query can still result in charges. You're charged for the amount of evidence data that was scanned before you stopped the search query. After it's stopped, you can view the partial results that were returned.

To stop an in-progress search query

1. In the blue progress flash bar at the top of the screen, choose **Stop search**.



2. (Optional) Review the partial results that were returned before you stopped the search query.
   a. If you're on the evidence finder page, the partial results are displayed on the screen.
   b. If you navigated away from evidence finder, choose **View partial results** in the green confirmation flash bar.

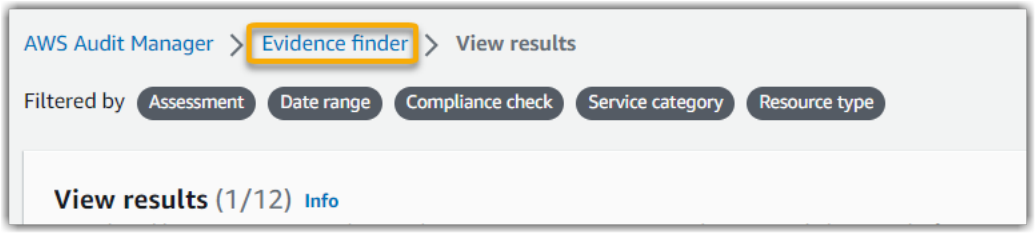
Editing search filters

Follow these steps to return to your most recent search query and adjust the filters as needed.

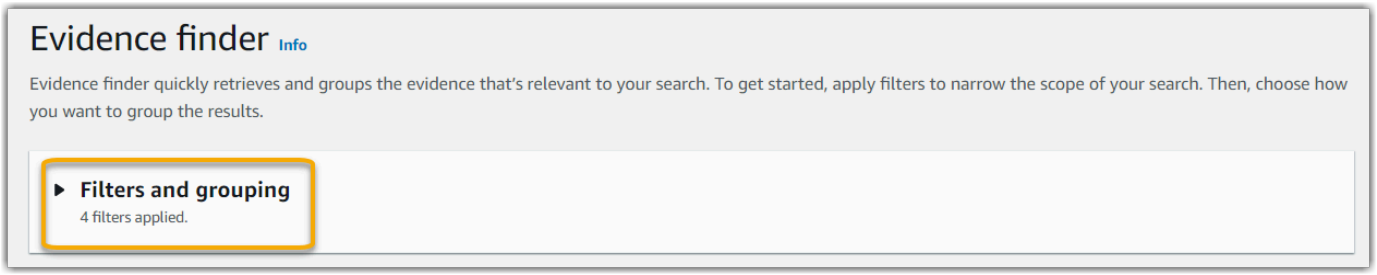
> **Note**
>
> When you edit your filters and choose **Search**, this starts a new search query.

To edit a recent search query

1. From the **View results** page, choose **Evidence finder** from the breadcrumb navigation menu.



2. Choose **Filters and grouping** to expand the filter selection.



3. Next, edit your filters or start a new search.

   a. To edit filters, adjust or remove the current filters and grouping selection.

   b. To start over, choose **Clear filters** and apply the filters and grouping selection of your choice.

4. When you're done, choose **Search**.

Next steps

After your search is finished, you can view the results that matched your search criteria. For instructions, see Viewing results in evidence finder.

Additional resources

- Filter and grouping options for evidence finder
- Example use cases for evidence finder
- Troubleshooting evidence finder issues

Viewing results in evidence finder

After your search is finished, you can view the results that matched your search criteria.

Keep in mind that multiple resources might be assessed during evidence collection. As a result, evidence can include one or more related resources. In evidence finder, results are shown at the resource level, with one row for each resource. You can preview a summary of each resource without leaving the page.

After you review the search results, you can generate an assessment report that includes that evidence. You can also export your search results into a comma-separated values (CSV) file.

Important

We recommend that you keep evidence finder open until you finished exploring your search results. Your search results are discarded when you navigate away from the **View Results** table. If needed, you can view your recent results in the CloudTrail console at https://console.aws.amazon.com/cloudtrail/. Here, the results of your search queries are preserved for seven days. However, keep in mind that you can't generate an assessment report from your search results in the CloudTrail console.

Prerequisites

The following procedure assumes that you already followed the steps to perform a search in evidence finder.

Procedure

Follow these steps to view your search results in evidence finder.

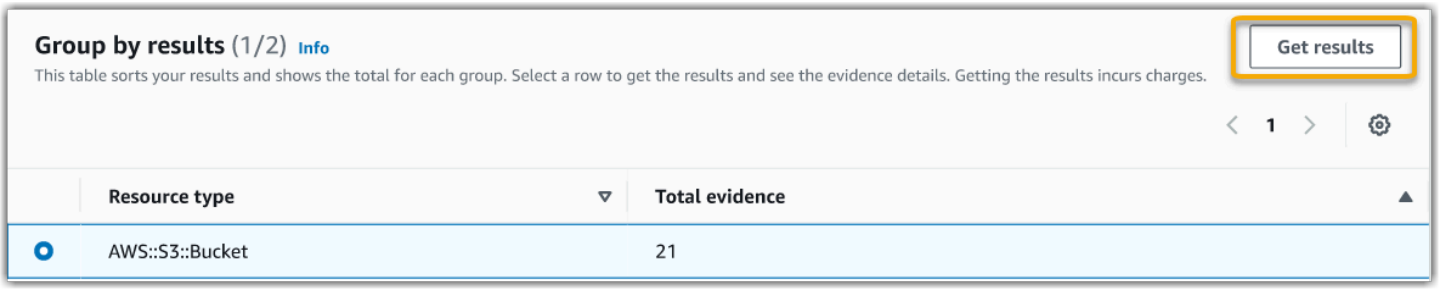
Tasks

Step 1. Viewing the grouped results

If you grouped your results, you can review the groupings before you dive deeper into the evidence.

> **Note**
>
> If you didn't group results, evidence finder doesn't display the **Group by results** table. Instead, you're taken directly to the **View results** table.

Use the **Group by results** table to learn the breadth of the matching evidence and how it's distributed across a specific dimension. Results are grouped by the value that you selected. For example, if you grouped by **Resource type**, the table shows a list of AWS resource types. The **Total evidence** column shows the number of matching results for each resource type.



To get the results for a group

1. From the **Group by results** table, select the row for the results that you want to get.
2. Choose **Get results**. This starts a new search query, and redirects you to the **View results** table where you can see the results for that group.

Step 2. Viewing the search results

The **View results** table displays your search results. From here, you can manage your viewing preferences and preview resource summaries.

Managing your viewing preferences

Your viewing preferences control what you see on the results page.

To manage your viewing preferences

1. Choose the settings icon (#) at the top of the **View results** table.
2. Review and change the following settings as needed:

Setting	Description
Select visible table columns	Use the toggle option to change which columns are displayed.
Page size	Select a radio button to specify how many results are shown on each page.
Wrap text	Select the check box to wrap long lines of text for better readability.

3. Choose **Confirm** to save your preferences.

Previewing resource summaries

You can preview the related resources for the evidence that matched your search query. This helps you determine if the search query returned the intended results, or if you need to adjust your filters and re-run the search query.

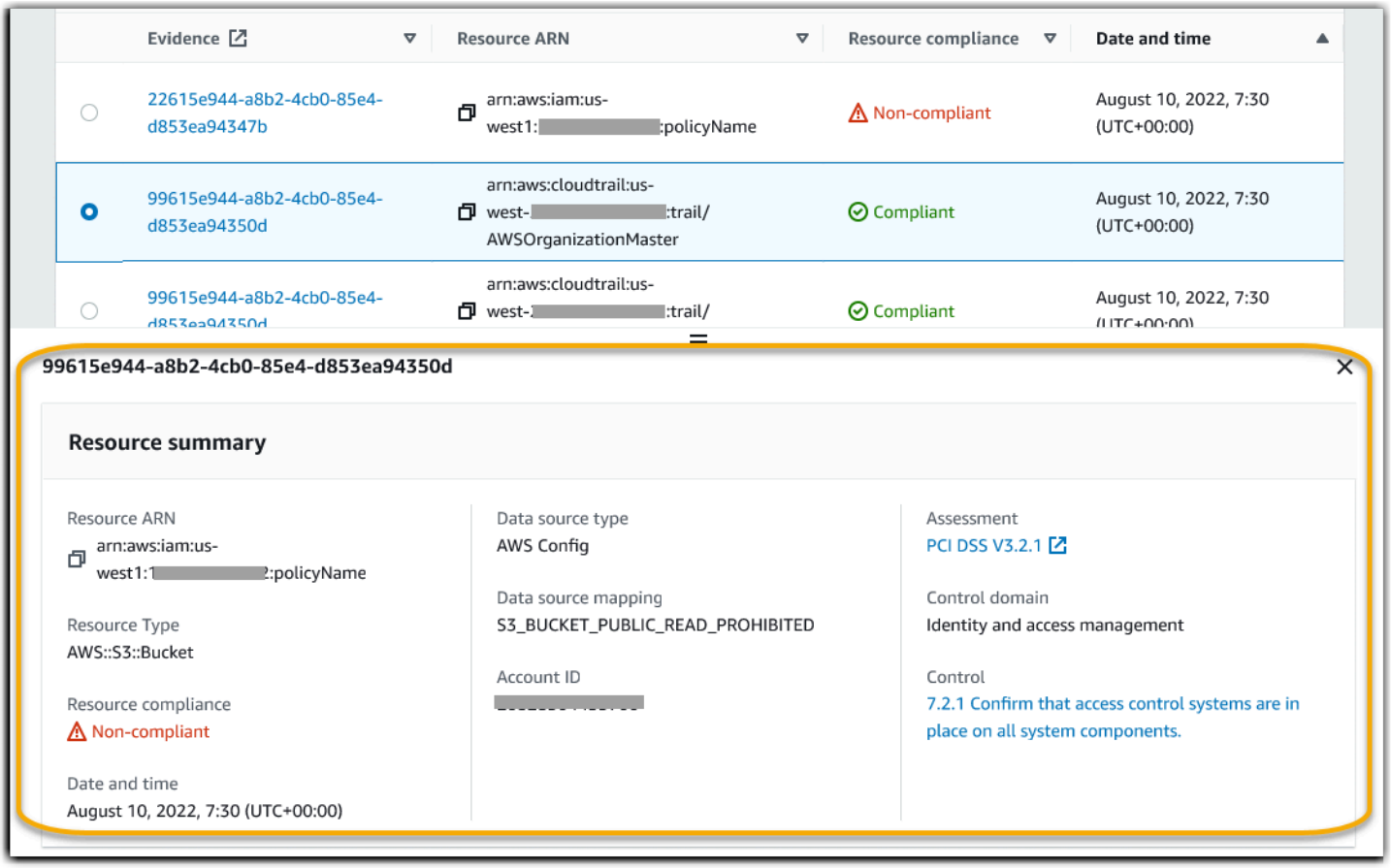
Keep in mind that evidence can have one or more related resources. Evidence finder shows results at the resource level (with one row for each resource).

> **Note**
>
> Evidence finder returns results for automated and manual evidence. However, you can only preview resource summaries for automated evidence. This is because Audit Manager

doesn't perform resource assessments for manual evidence, and as a result, no resource summary is available.
To see details about manual evidence, choose the evidence name to open the evidence details page. If you generate an assessment report from your evidence finder results, the manual evidence details are included in the assessment report.

To preview resource summaries

1. Select the radio button next to a result. This opens a resource summary panel on the current page.
2. (Optional) To see the full details of the related evidence, choose the evidence name.
3. (Optional) Use the horizontal lines (**=**) to drag and resize the resource summary pane.
4. Choose (**x**) to close the resource summary pane.



Next steps

After you review your search results, you can generate an assessment report from them or export them as a CSV file. For instructions, see Exporting your search results from evidence finder.

Additional resources

- Filter and grouping options for evidence finder
- Example use cases for evidence finder
- Troubleshooting evidence finder issues

Exporting your search results from evidence finder

After you've reviewed your search results, you can generate an assessment report based on those results. Alternatively, you can export your evidence finder search results in a CSV file.

Prerequisites

The following procedure assumes that you already followed the steps to perform a search and review your search results in evidence finder.

Procedure

Contents

Generating an assessment report from your search results

After you're satisfied with the search results, you can generate an assessment report.

To generate an assessment report from your search results

1. At the top of the **View results** table, choose **Generate assessment report**.

2. Enter a name and a description for your assessment report, and review the assessment report details.
3. Choose **Generate assessment report**.

It takes a few minutes for your assessment report to be generated. You can navigate away from evidence finder while this happens, and a green success notification will confirm when the report is ready. You can then go to the Audit Manager download center and download your assessment report.

> **Note**
>
> Audit Manager generates a one-time report using only the evidence from the search results. This report doesn't include any evidence that was manually added to a report from the assessment page.
> Limits apply to how much evidence can be included in an assessment report. For more information, see Troubleshooting evidence finder issues.

Exporting your search results into a CSV file

You might need a portable version of your evidence finder search results. If this is the case, you can export your search results into a CSV file.

After you export your search results, the CSV file is available in the Audit Manager download center for seven days. A copy of the CSV file is also delivered to your preferred S3 bucket, which is known as an *export destination*. Your CSV file remains available in this bucket until you delete that file.

Audit Manager uses CloudTrail Lake functionality to export and deliver CSV files from evidence finder. The following factors define how the CSV export process works:

- All of your search results are included in the CSV file. If you want to include only specific search results, we recommend that you edit your search filters. This way, you can narrow down your results to target only the evidence that you want to export.
- CSV files are exported in compressed GZIP format. The default CSV file name is `queryID/result.csv.gz`, where `queryID` is the ID of your search query.
- The maximum file size for a CSV export is 1 TB. If you're exporting over 1 TB of data, your results are split into more than one file. Each CSV file is named `result_`*`number`*`.csv.gz`. The number of CSV files that you get depends on the total size of your search results. For

example, exporting 2 TB of data provides you with two query result files: `result_1.csv.gz` and `result_2.csv.gz`.

- In addition to the CSV file, a JSON sign file is delivered to your S3 bucket. This file acts as a checksum to verify that the information within the CSV file is accurate. To learn more, see CloudTrail sign file structure in the *AWS CloudTrail Developer Guide*. To determine whether the query results were modified, deleted, or unchanged after they were delivered, you can use the CloudTrail query results integrity validation. For instructions, see Validate saved query results in the *AWS CloudTrail Developer Guide*.

> **Note**
>
> Manual evidence text responses are not currently included in evidence finder previews or CSV exports. To see text response data, choose the manual evidence name in your evidence finder results to open the evidence details page. If you need to view text response data outside of the Audit Manager console, we recommend that you generate an assessment report from your evidence finder results. All manual evidence details, including text responses, are included in assessment reports.

Exporting your results for the first time

Follow these steps to export your search results for the first time. This procedure gives you the option to specify a default export destination for all of your future exports. If you don't want to save a default export destination right now, you can do so later by updating your export destination settings.

> **Important**
>
> Before you start, make sure that you have an S3 bucket available to use as your export destination. You can use one of your existing S3 buckets, or you can create a new bucket in Amazon S3. For optimal security and performance, we recommend using an S3 bucket in the same AWS account and region as your assessment. In addition, your S3 bucket must have the required permissions policy to allow CloudTrail to write the export files to it. More specifically, the bucket policy must include an `s3:PutObject` action and the bucket ARN, and list CloudTrail as the service principal. We provide an example permission policy that you can use. For instructions on how to attach this policy to your S3 bucket, see Adding a bucket policy by using the Amazon S3 console.

For more tips, see Configuration tips for your export destination. If you encounter any issues when exporting a CSV file, see csv-exports.

To export your search results (first-run experience)

1. At the top of the **View results** table, choose **Export CSV**.
2. Specify the S3 bucket that you want to export your file to.
   - Choose **Browse S3** to select from your list of buckets.
   - Alternatively, you can enter the bucket URI in this format: **`s3://bucketname/prefix`**

   Tip

   To keep your destination bucket organized, you can create an optional folder for your CSV exports. To do so, append a slash (**/**) and a prefix to the value in the **Resource URI** box (for example, **`/evidenceFinderExports`**). Audit Manager then includes this prefix when it adds the CSV file to the bucket, and Amazon S3 generates the path specified by the prefix. For more information about prefixes in Amazon S3, see Organizing objects in the Amazon S3 console in the *Amazon Simple Storage Service* User Guide.
3. (Optional) If you don't want to save this bucket as your default export destination, clear the check box that says **Save this bucket as the default export destination in my evidence finder settings**.
4. Choose **Export**.

Exporting your results after you've saved an export destination

After you've saved a default S3 bucket as your default export destination, you can follow these steps moving forward.

To export your search results (after you saved a default export destination)

1. At the top of the **View results** table, choose **Export CSV**.
2. In the prompt that appears, review the default S3 bucket where your exported file will be saved.

   a. (Optional) To continue using this bucket and hide this message moving forward, check the **Don't remind me again** box.
   b. (Optional) To change this bucket, follow the procedure to update your export destination settings.
3. Choose **Confirm**.

Depending on how much data you're exporting, the export process can take a few minutes to complete. You can navigate away from evidence finder while the export is in progress. When you navigate away from evidence finder, your search is stopped and your search results are discarded in the console. However, the CSV export process continues in the background. The CSV file will contain the complete set of search results that matched your query.

Viewing your results after you've exported them

To find your CSV file and check its status, go to the Audit Manager Audit Manager download center. When the exported file is ready, you can download your CSV file from the download center.

You can also find and download the CSV file from your export destination S3 bucket.

To find your CSV file and sign file in the Amazon S3 console

1. Open the Amazon S3 console.
2. Choose the export destination bucket that you specified when you exported your CSV file.
3. Navigate through the object hierarchy until you find the CSV file and the sign file. The CSV file has a `.csv.gz` extension and the sign file has a `.json` extension.

You will navigate through an object hierarchy that is similar to the following example, but with a different export destination bucket name, account ID, date, and query ID.

```
All Buckets
    Export_Destination_Bucket_Name
        AWSLogs
            Account_ID;
                CloudTrail-Lake
                    Query
                        YYYY
                            MM
                              DD
```

```
Query_ID
```

Additional resources

- Troubleshooting evidence finder issues
- Configuring your default export destination for evidence finder

Filter and grouping options for evidence finder

On this page, you can see a list of the filter and grouping options that are available for you to use in evidence finder.

Filter reference

You can use the following filters to find evidence that matches specific criteria, such as an assessment, control, or AWS service.

Topics

Required filters

Use these filters to get started with a high-level overview of the evidence in an assessment.

Filter name	Description	Notes
Assessment	Returns evidence for a specific assessment.	You can filter by one assessment only.
Date range	Returns evidence for a specific time period.	Either, you can use a *Relative range* to define a range that's relative to today's date (for example, **`Last 30 days`**).

Filter name	Description	Notes
		Or, you can use an *Absolute range* to specify a specific date range (for example, **`June 27th - July 4th`**).
Resource compliance	Returns resources with a specific compliance check evaluation.	Audit Manager collects compliance check evidence for controls that use AWS Config and Security Hub as a data source type. Multiple resources might be assessed during evidence collection. As a result, a single piece of compliance check evidence can include one or more resources. You can use this filter to explore compliance status at the resource level. You can choose one or more of the following options: • **Non-compliant** – This filter finds resources with compliance check issues. This happens if Security Hub reports a *Fail* result, or if AWS Config reports a *Non-compliant* result. • **Compliant** – This filter finds resources that don't have compliance check issues. This happens if Security Hub reports a *Pass* result, or if AWS Config reports a *Compliant* result. • **Inconclusive** – This filter finds resources for which a compliance check isn't available or applicable. This happens if a resource uses AWS Config or Security Hub as the underlyin g data source type, but those services aren't enabled. This also happens if the resource uses an underlying data source type that doesn't support compliance checks (such as manual evidence, AWS API calls, or CloudTrail).

Additional filters (optional)

Use these filters to narrow the scope of your search query. For example, use **Service** to see all evidence that's related to Amazon S3. Use **Resource type** to focus just on S3 buckets. Or, use **Resource ARN** to target a specific S3 bucket.

You can create additional filters using one or more of the following criteria.

Criteria name	Description	When to use this criteria
Account ID	Drill down by AWS account.	Use this criteria to find evidence that's related to a specific AWS account.
Control	Drill down by control name.	Use this criteria to find evidence that's related to a specific control.
Control domain	Drill down by control domain.	Use this criteria to focus on a specific subject area as you prepare for an audit. You can filter by control domain if you're querying an assessment that was created from a standard framework. Examples of control domains include network security, identity and access management, and data protection. Some control domains might be marked as **Outdated** following Audit Manager's transition to a new set of control domains provided by AWS Control Catalog. For more information, see I see that a control domain is marked as “outdated”. What does this mean?.
Data source type	Drill down by the type of data source.	Use this criteria to focus on a specific data source. Set the value to `Manual` to find evidence that you uploaded manually. Otherwise, you can filter automated evidence based on where it came from (for example, `AWS Config`, `CloudTrail` , `Security Hub`, or `AWS API calls`).

Criteria name	Description	When to use this criteria
Event name	Drill down by event name.	Use this criteria to focus on a specific event that the evidence is related to. An event is a record of an activity in an AWS account. For example, you can search for the name of an API call, such as the IAM `AttachRolePolicy` operation that's used to configure permissions. Or, search for a CloudTrail keyword, such as the `ConsoleLogin` event that's logged by CloudTrail when a user signs in to your account.
Resource ARN	Drill down by Amazon Resource Name (ARN).	Use this criteria to find evidence that's related to a specific AWS resource.
Resource type	Drill down by resource type.	Use this criteria to focus on the type of resource that's being assessed, such as an Amazon EC2 instance or an S3 bucket.
Service	Drill down by AWS service name.	Use this criteria to find evidence that's related to a specific AWS service, such as Amazon EC2, Amazon S3, or AWS Config.
Service category	Drill down by AWS service category.	Use this criteria to focus on a specific category of AWS service. Examples include security, identity and compliance, database, and storage.

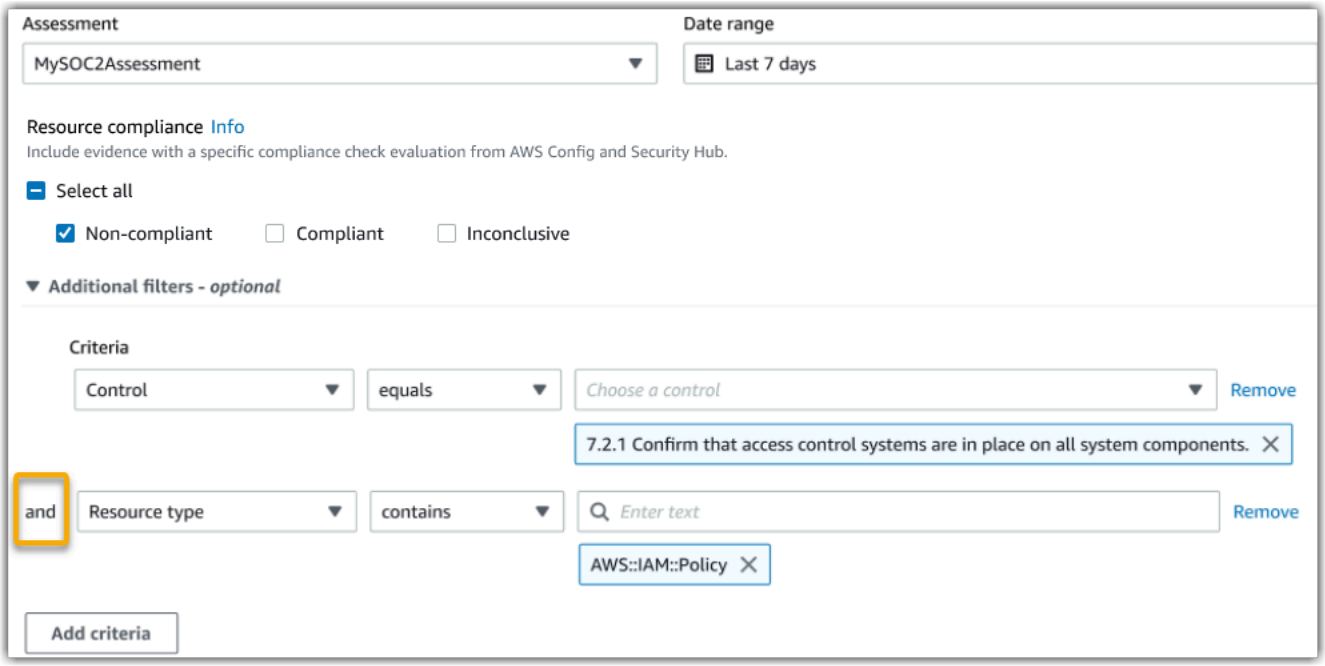
Combining filters

Criteria behavior

When you specify more than one criteria, Audit Manager applies the `AND` operator to your selections. This means that all of the criteria are grouped into a single query, and the results must match all of the combined criteria.

Example

In the following filter setup, evidence finder returns non-compliant resources from the last 7 days for the assessment that's called **`MySOC2Assessment`**. Additionally, the results relate to both an IAM policy and the specified control.

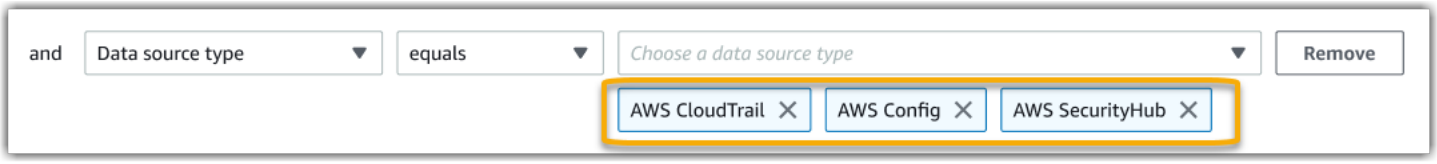


Criteria value behavior

When you specify more than one criteria value, the values are linked with an OR operator. Evidence finder returns results that match any of these criteria values.

Example

In the following filter setup, evidence finder returns search results that come from either AWS CloudTrail, AWS Config, or AWS Security Hub.



Grouping reference

You can group your search results for quicker navigation. Grouping shows you the breadth of your search results, and how they're distributed across a specific dimension.

You can use any of the following group by values.

Group by	Description
Account ID	Group results by AWS account.
Control	Group results by control name.
Data source type	Group results by the type of data source where the evidence came from.
Event name	Group results by an event name.
Resource ARN	Group results by Amazon Resource Name (ARN).
Resource type	Group results by resource type.
Service	Group results by AWS service name.
Service category	Group results by AWS service category.

Example use cases for evidence finder

Evidence finder can help you with several use cases. This page provides some examples and suggests the search filters that you can use in each scenario.

Topics

Use case 1: Find non-compliant evidence and organize delegations

This use case is ideal if you're a compliance officer, a data protection officer, or a GRC professional who oversees audit preparation.

As you monitor the compliance posture for your organization, you might rely on partner teams to help you remediate issues. You can use evidence finder to help you organize your work for your partner teams.

By applying filters, you can focus on evidence for one area at a time. Moreover, you can also stay aligned with the responsibilities and scope of each partner team that you work with. By performing a targeted search in this way, you can use the search results to identify what exactly needs remediating in each subject area. You can then delegate that non-compliant evidence to the corresponding partner team for remediation.

For this workflow, follow the steps to search for evidence. Use the following filters to find non-compliant evidence.

```
Assessment | <assessment name>
Date range | <date range>
Resource compliance | Non-compliant
```

Next, apply additional filters for the area that you're focusing on. For example, use the **Service category** filter to find non-compliant resources that are related to IAM. Then, share those results with the team that owns IAM resources for your organization. Or, if you're querying an assessment that was created from a standard framework, you can use the **Control domain** filter to find non-compliant evidence that's related to the identity and access management domain.

```
Control domain | <domain that you're focusing on>
or
Service category | <AWS service category that you're focusing on>
```

After you find the evidence that you need, follow the steps to generate an assessment report from your search results. For instructions, see Generating an assessment report from your search results. You can share this report with your partner team, who can use it as a remediation checklist.

Use case 2: Identify compliant evidence

This use case is ideal if you work in SecOps, IT/DevOps, or another role that owns and remediates cloud assets.

As part of an audit, you might be asked to remediate issues with the resources that you own. After you do this work, you can use evidence finder to validate that your resources are compliant.

For this workflow, follow the steps to search for evidence. Use the following filters to find compliant evidence.

```
Assessment | <assessment name>
```

```
Date range | <date range>
Resource compliance | Compliant
```

Next, apply additional filters to show only the evidence that you're responsible for. Depending on your ownership scope, make the search as targeted as needed. The following filter examples are ordered from broadest to most precise. Choose the appropriate options for you, and replace the *<placeholder text>* with your own values.

```
Control domain | <a subject area that you're responsible for>
Service category | <a category of AWS services that you own>
Service | <a specific AWS service that you own>
Resource type | <a collection of resources that you own>
Resource ARN | <a specific resource that you own>
```

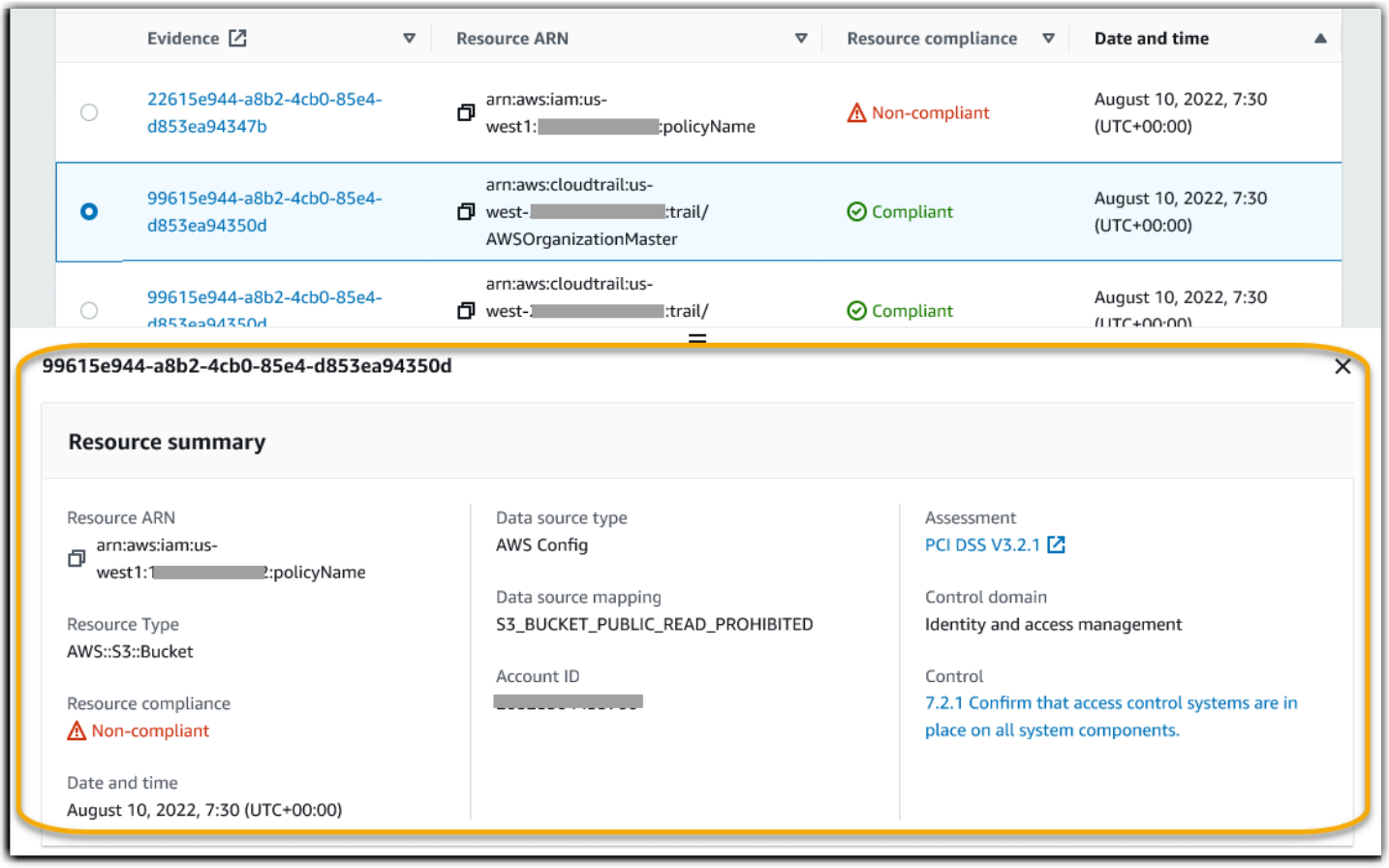
If you're responsible for multiple instances of the same criteria (for example, you own multiple AWS services), you can group your results by that value. This provides you with the total evidence matches for each AWS service. You can then get the results for the services that you own.

Use case 3: Perform a quick preview of evidence resources

This use case is ideal for all Audit Manager customers.

Previously, it was time consuming to review individual evidence details. If you wanted to preview evidence, you had to go directly to that assessment, then navigate through deeply nested evidence folders. Now, evidence finder provides a convenient way to preview this information. For each evidence item that matches your search query, you can preview the individual resources for that evidence.

To get started, follow the steps to search for evidence. Then, select the radio button next to a result to see a resource summary in the current page. You can preview each individual resource that relates to an evidence item. To see the full evidence details for any resource, choose the evidence name. For more information, see Previewing resource summaries.


Evidence
Resource ARN
Resource compliance
Date and time
22615e944-a8b2-4cb0-85e4-d853ea94347b
arn:aws:iam:us-west1:[redacted]:policyName
Non-compliant
August 10, 2022, 7:30 (UTC+00:00)
99615e944-a8b2-4cb0-85e4-d853ea94350d
arn:aws:cloudtrail:us-west-[redacted]:trail/AWSOrganizationMaster
Compliant
August 10, 2022, 7:30 (UTC+00:00)
99615e944-a8b2-4cb0-85e4-d853ea94350d
arn:aws:cloudtrail:us-west-[redacted]:trail/
Compliant
August 10, 2022, 7:30
99615e944-a8b2-4cb0-85e4-d853ea94350d
Resource summary
Resource ARN
arn:aws:iam:us-west1:[redacted]:policyName
Resource Type
AWS::S3::Bucket
Resource compliance
Non-compliant
Date and time
August 10, 2022, 7:30 (UTC+00:00)
Data source type
AWS Config
Data source mapping
S3_BUCKET_PUBLIC_READ_PROHIBITED
Account ID
[redacted]
Assessment
PCI DSS V3.2.1
Control domain
Identity and access management
Control
7.2.1 Confirm that access control systems are in place on all system components.

Audit Manager download center

The download center is where you can find and manage all of your downloadable Audit Manager files. When you generate an assessment report or export search results from evidence finder, the files appear in the download center.

Contents

Browsing the download center

Follow these steps to browse your files in the download center.

To find files in the download center

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the left navigation pane, choose **Download center**.
3. Choose the **Assessment reports** tab to view the assessment reports that are available to download.

   - This tab shows the assessment reports that you've generated. Assessment reports remain available in the download center until you delete them.
   - To see the latest status of your assessment report, choose the refresh icon (#) to reload the table. Each row in the assessment reports table shows the name of the report, its creation date, and one of the following statuses:

Status	Description
In progress	Audit Manager is generating the assessment report.
Ready	The assessment report is available for you to download.

Status	Description
Error	The assessment report failed to generate. In this case, Audit Manager displays a message that describes the error. For information about how to resolve these errors, see Troubleshooting assessment report issues.

4. Choose the **Exports** tab to view the CSV exports that are available to download.

   - This tab shows the evidence finder search results that you exported in the last seven days. CSV files are removed from the download center after seven days, but they remain available in your export destination S3 bucket. For instructions on how to find an evidence finder CSV export in your S3 destination bucket, see Viewing your results after you've exported them.
   - To see the latest status of your CSV exports, choose the refresh icon (#) to reload the table. Each row in the exports table shows the file name, its export date, and one of the following statuses:

Status	Description
In progress	Audit Manager is preparing the CSV file.
Ready	The export succeeded and the file is available for you to download.
Error	The export failed. In this case, Audit Manager displays a message that describes the error. For information about how to resolve these errors, see csv-exports.

> **Note**
>
> Keep in mind that the exports tab might also display CSV files for queries that you ran directly in AWS CloudTrail Lake. This includes queries made in the CloudTrail console or using the CloudTrail API. CloudTrail exports appear on this tab if you

queried the Audit Manager event data store, and you chose to save the results to Amazon S3.

Downloading a file

Follow these steps to download a file from the download center.

To download a file

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the left navigation pane, choose **Download center**.
3. Choose either the **Assessment reports** tab or the **Exports** tab.
4. Select the file that you want to download, and choose **Download**.

For instructions on how to download a file directly from your S3 destination bucket, see Downloading an object in the *Amazon Simple Storage Service (Amazon S3) User Guide*.

Deleting a file

Follow these steps to delete any assessment reports that you no longer need in the download center.

Note

Deleting CSV exports from the download center isn't currently supported. CSV exports are automatically removed from the download center after seven days.

To delete an assessment report

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the left navigation pane, choose **Download center**.
3. Choose the **Assessment reports** tab.

4. Select the assessment report that you want to delete, and choose **Delete**.

If you want to delete an assessment report or a CSV export from your S3 destination bucket, we recommend that you complete this task directly in Amazon S3. For instructions, see Deleting Amazon S3 objects in the *Amazon Simple Storage Service (Amazon S3) User Guide*.

Additional resources

- Configuring your default export destination for evidence finder
- Configuring your default assessment report destination
- Troubleshooting assessment report issues
- Troubleshooting CSV export issues
- Downloading an object from Amazon S3
- Deleting Amazon S3 objects

Using the framework library to manage frameworks in AWS Audit Manager

You can find and manage frameworks in the framework library in AWS Audit Manager.

A framework determines which controls are tested in an environment over a period of time. It defines the controls and their data source mappings for a given compliance standard or regulation. It's also used to structure and automate Audit Manager assessments. You can use frameworks as a starting point to audit your AWS service usage and start automating evidence collection.

Key points

In the framework library, frameworks are organized into the following categories.

- **Standard frameworks** are prebuilt frameworks that AWS provides. These frameworks are based on AWS best practices for different compliance standards and regulations, such as GDPR and HIPAA. Standard frameworks include controls that are organized into control sets based on the compliance standard or regulation that the framework supports.

  You can view the contents of standard frameworks, but you can't edit or delete them. However, you can make an editable copy of any standard framework to create a new one to meet your specific requirements.
- **Custom frameworks** are frameworks that you create. You can create a custom framework from scratch, or by making an editable copy of an existing framework. You can use custom frameworks to organize controls into control sets in a way that meets your specific requirements.

You can create an assessment from a standard framework or a custom framework.

> **Note**
>
> AWS Audit Manager assists in collecting evidence that's relevant for verifying compliance with specific compliance standards and regulations. However, it doesn't assess your compliance itself. The evidence that's collected through AWS Audit Manager therefore might not include all the information about your AWS usage that's needed for audits. AWS Audit Manager isn't a substitute for legal counsel or compliance experts.

Additional resources

To create and manage frameworks in Audit Manager, follow the procedures that are outlined here.

- Finding the available frameworks in AWS Audit Manager
- Reviewing a framework in AWS Audit Manager
- Creating a custom framework in AWS Audit Manager
  - Creating a custom framework from scratch in AWS Audit Manager
  - Making an editable copy of an existing framework in AWS Audit Manager
- Editing a custom framework in AWS Audit Manager
- Deleting a custom framework in AWS Audit Manager
- Sharing a custom framework in AWS Audit Manager
  - Framework sharing concepts and terminology
  - Sending request to share a custom framework in AWS Audit Manager
  - Responding to share requests in AWS Audit Manager
  - Deleting share requests in AWS Audit Manager
- Supported frameworks in AWS Audit Manager

Finding the available frameworks in AWS Audit Manager

You can find all available frameworks on the **Framework library** page in the Audit Manager console.

You can also view all available frameworks using the Audit Manager API or the AWS Command Line Interface (AWS CLI).

Prerequisites

Make sure your IAM identity has appropriate permissions to view frameworks in AWS Audit Manager. Two suggested policies that grant these permissions are AWSAuditManagerAdministratorAccess and Allow users management access to AWS Audit Manager.

Procedure

Audit Manager console

To view available frameworks on the Audit Manager console

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the left navigation pane, choose **Framework library**.
3. Choose the **Standard frameworks** tab or the **Custom frameworks** tab to browse the available standard and custom frameworks.

AWS CLI

To view available frameworks in the AWS CLI

To view frameworks in Audit Manager, use the list-assessment-frameworks command and specify a `--framework-type`. Either, you can retrieve a list of standard frameworks. Or, you can retrieve a list of custom frameworks.

```
aws auditmanager list-assessment-frameworks --framework-type Standard
```

```
aws auditmanager list-assessment-frameworks --framework-type Custom
```

Audit Manager API

To view available frameworks using the API

Use the ListAssessmentFrameworks operation and specify a frameworkType. Either, you can return a list of standard frameworks. Or, you can return a list of custom frameworks.

For more information, choose either of the previous links to read more in the *AWS Audit Manager API Reference*. This includes information about how to use the `ListAssessmentFrameworks` operation and parameters in one of the language-specific AWS SDKs.

Next steps

When you're ready to explore the details of a framework, follow the steps in Reviewing a framework in AWS Audit Manager. This page will guide you through the framework details and explain the information that you see there.

From the framework library page, you can also create, edit, delete, or share a custom framework.

Additional resources

For solutions to framework issues in Audit Manager, see Troubleshooting framework issues.

Reviewing a framework in AWS Audit Manager

You can review the details of a framework using the Audit Manager console, the Audit Manager API, or the AWS Command Line Interface (AWS CLI).

Prerequisites

Make sure your IAM identity has appropriate permissions to view frameworks in AWS Audit Manager. Two suggested policies that grant these permissions are AWSAuditManagerAdministratorAccess and Allow users management access to AWS Audit Manager.

Procedure

Audit Manager console

To view framework details on the Audit Manager console

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the left navigation pane, choose **Framework library** to see a list of available frameworks.
3. Choose the **Standard frameworks** tab or the **Custom frameworks** tab to browse the available frameworks.
4. Choose the name of the framework to open it.

5. Review the framework details using the following information as reference.

Framework details section

This section provides an overview of the framework. In this section, you can review the following information:

Name	Description
Description	A description of the framework, if one was provided.
Framework type	Specifies whether the framework is a standard framework or a custom framework.
Compliance type	The compliance standard or regulation that the framework supports.

If you're viewing a custom framework, you can also see the following details:

Name	Description
Created by	The account that created the custom framework.
Date created	The date when the custom framework was created.
Last updated	The date when this framework was last edited.

Controls tab

This tab lists the controls in the framework, grouped by control set. On this tab, you can review the following information:

Name	Description
Controls grouped by control set	Choose the tree view icon to see the controls that belong to each control set.

Name	Description
Type	Specifies whether the control is a standard control or a custom control.
Data sources	Specifies the data source where Audit Manager collects evidence from for that framework control.

Tags tab

This tab lists the tags that are associated with the framework. On this tab, you can review the following information:

Name	Description
Key	The tag key (for example, a compliance standard, regulation, or category).
Value	The tag value.

AWS CLI

To view framework details in the AWS CLI

1. To identify the framework that you want to review, run the list-assessment-frameworks command and specify a `--framework-type`. Either, you can retrieve a list of standard frameworks. Or, you can retrieve a list of custom frameworks.

   In the following example, replace the *`placeholder text`* with either `Custom` or `Standard`.

   ```
   aws auditmanager list-assessment-frameworks --framework-type Custom/Standard
   ```

   The response returns a list of frameworks. Find the framework that you want to review, and take note of the framework ID and Amazon Resource Name (ARN).
2. To get the framework details, run the get-assessment-framework command and specify the `--framework-id`.

In the following example, replace the *placeholder text* with your own information.

```
aws auditmanager get-assessment-framework --framework-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

> **Tip**
>
> The framework details are returned in JSON format. To understand this data, see get-assessment-framework Output in the *AWS CLI Command Reference*.

3. To see the tags for a framework, use the list-tags-for-resource command and specify the `--resource-arn` for the framework.

   In the following example, replace the *placeholder text* with your own information:

   ```
   aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:assessmentFramework/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

   For more information about tags in Audit Manager, see Tagging AWS Audit Manager resources.

Audit Manager API

To view framework details using the API

1. To identify the framework that you want to review, use the ListAssessmentFrameworks operation and specify a frameworkType. Either, you can return a list of standard frameworks. Or, you can return a list of custom frameworks.

   From the response, find the framework that you want to review and note the framework ID and Amazon Resource Name (ARN).

2. To get the framework details, use the GetAssessmentFramework operation. In the request, specify the frameworkId that you got from step 1.

> **Tip**
>
> The framework details are returned in JSON format. To understand this data, see GetAssessmentFramework Response Elements in the *AWS Audit Manager API Reference*.

3. To see tags for the framework, use the ListTagsForResource operation. In the request, specify the framework resourceArn that you got from step 1.

For more information about tags in Audit Manager, see Tagging AWS Audit Manager resources.

For more information about these API operations, choose any of the links in the previous procedure to read more in the *AWS Audit Manager API Reference*. This includes information about how to use these operations and parameters in one of the language-specific AWS SDKs.

Next steps

From the framework details page, you can create an assessment from the framework or make an editable copy of the framework.

If you're reviewing a custom framework, you can also edit, delete, or share the framework.

Additional resources

- On my custom framework details page, I'm prompted to recreate my custom framework
- I can't make a copy of my custom framework

Creating a custom framework in AWS Audit Manager

You can use custom frameworks to organize controls into control sets in a way that meets your specific requirements.

Key points

When it comes to creating custom frameworks in Audit Manager, you have two methods to choose from:

1. **Creating a custom framework from scratch** - This gives you the flexibility to start with a clean slate and define every aspect of the framework according to your specifications. This approach is particularly beneficial when your requirements deviate significantly from existing standard frameworks, or when you need to incorporate proprietary control sets specific to your organization.
2. **Making an editable copy of an existing framework** - This approach enables you to leverage the structure and content of an existing framework while providing the freedom to customize it to suit your specific needs. By starting with an established foundation, you can streamline the process of building your custom framework, focusing your efforts on tailoring it to your organization's unique requirements.

Regardless of the approach you choose, creating a custom framework involves a series of steps such as specifying framework details, defining control sets, and reviewing the framework before finalizing its creation. Throughout this process, you can incorporate your organization's specific control sets, ensuring that the custom framework accurately reflects your GRC requirements.

Additional resources

For instructions on how to create a custom framework, see the following resources.

- Creating a custom framework from scratch in AWS Audit Manager
- Making an editable copy of an existing framework in AWS Audit Manager

Creating a custom framework from scratch in AWS Audit Manager

When your organization's compliance requirements don't align with the pre-built standard frameworks that are available in AWS Audit Manager, you can create your own custom framework from scratch instead.

This page outlines the steps to create a custom framework that's tailored to your specific needs.

Prerequisites

Make sure your IAM identity has appropriate permissions to create a custom framework in AWS Audit Manager. Two suggested policies that grant these permissions are AWSAuditManagerAdministratorAccess and Allow users management access to AWS Audit Manager.

Procedure

Tasks

- Step 1: Specify framework details
- Step 2: Specify control sets
- Step 3: Review and create the framework

Step 1: Specify framework details

Start by specifying details about your custom framework.

To specify framework details

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the left navigation pane, choose **Framework library** and then choose **Create custom framework**.
3. Under **Framework details**, enter a name, a compliance type (optional), and a description for your framework (also optional). Entering a compliance type such as *PCI_DSS* or *GDPR* means you can use this keyword to search for your framework later.
4. Under **Tags**, choose **Add new tag** to associate a tag with your framework. You can specify a key and a value for each tag. The tag key is mandatory. You can use it as search criteria when searching for this framework in the framework library.
5. Choose **Next**.

Step 2: Specify control sets

Next, you specify which controls you want add to your framework and how you want to organize them. Start by adding control sets to the framework, and then add controls to the control set.

> **Note**
>
> When you use the AWS Audit Manager console to create a custom framework, you can add up to 10 control sets for each framework.

When you use the Audit Manager API to create a custom framework, you can create more than 10 control sets. To add more control sets than the console currently allows, use the CreateAssessmentFramework API that Audit Manager provides.

To specify a control set

1. Under **Control set name**, enter a name for your control set.
2. Under **Add controls**, use the **Control type** dropdown list to select one of the two control types: **Standard controls** or **Custom controls**.
3. Based on the option that you selected in the previous step, a list of standard controls or custom controls is displayed. Select one or more controls and choose **Add to control set**.
4. In the pop-up window that appears, choose **Add to control set**.
5. Review the controls that appear in the **Selected controls** list.
   - To add more controls, repeat steps 2–4.
   - To remove unwanted controls, select one or more controls and choose **Remove control**.
6. To add a new control set, choose **Add control set**.
7. To remove an unwanted control set, choose **Remove control set**.
8. After you finish adding control sets and controls, choose **Next**.

Step 3: Review and create the framework

Review the information for your framework. To change the information for a step, choose **Edit**.

When you're finished, choose **Create custom framework**.

Next steps

After you create your new custom framework, you can create an assessment from your framework. For more information, see Creating an assessment in AWS Audit Manager.

To revisit your custom framework at a later date, see Finding the available frameworks in AWS Audit Manager. You can follow these steps to locate your custom framework so that you can then view, edit, share, or delete it.

Additional resources

For solutions to framework issues in Audit Manager, see Troubleshooting framework issues.

Making an editable copy of an existing framework in AWS Audit Manager

Instead of creating a custom framework from scratch, you can use an existing framework as a starting point and make an editable copy. When you do this, the existing framework remains in the framework library, and a new custom framework is created with your specific settings.

You can make an editable copy of any existing framework. It can be either a standard framework or a custom framework.

Prerequisites

Make sure your IAM identity has appropriate permissions to create a custom framework in AWS Audit Manager. Two suggested policies that grant these permissions are AWSAuditManagerAdministratorAccess and Allow users management access to AWS Audit Manager.

Procedure

Tasks

- Step 1: Specify framework details
- Step 2: Specify control sets
- Step 3: Review and create the framework

Step 1: Specify framework details

All framework details, except tags, are carried over from the original framework. Review and modify these details as needed.

To specify framework details

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the left navigation pane, choose **Framework library**.

3. Choose the framework you want to use as a starting point, choose **Create custom framework**, and then choose **Make a copy**.
4. In the pop-up window that appears, enter a name for the new custom framework and choose **Continue**.
5. Under **Framework details**, review the name, compliance type, and description for your framework, and change them as needed. The compliance type should indicate the compliance standard or the regulation that's associated with your framework. You can use this keyword to search for your framework.
6. Under **Tags**, choose **Add new tag** to associate a tag with your framework. You can specify a key and a value for each tag. The tag key is mandatory and can be used as a search criteria when you search for this framework in the framework library.
7. Choose **Next**.

Step 2: Specify control sets

The control sets are carried over from the original framework. Change the current configuration by adding more controls or removing existing controls as needed.

> **Note**
>
> When you use the Audit Manager console to create a custom framework, you can add up to 10 control sets for each framework.
> When you use the Audit Manager API to create a custom framework, you can add more than 10 control sets. To add more control sets than the console currently allows, use the CreateAssessmentFramework API that Audit Manager provides.

To specify a control set

1. Under **Control set name**, change the name of the control set as needed.
2. Under **Add controls**, add a new control by using the dropdown list to select one of the two control types: **Standard controls** or **Custom controls**.
3. Based on the option that you selected in the previous step, a list of standard controls or custom controls is displayed. Select one or more controls and choose **Add to control set**.
4. In the pop-up window that appears, choose **Add to control set**.
5. Review the controls that appear in the **Selected controls** list.

- To add more controls, repeat steps 2–4.
- To remove unwanted controls, select one or more controls and choose **Remove control**.

6. To add a new control set to the framework, choose **Add control set**.
7. To remove an unwanted control set, choose **Remove control set**.
8. After you finish adding control sets and controls, choose **Next**.

Step 3: Review and create the framework

Review the information for your framework. To change the information for a step, choose **Edit**.

When you're finished, choose **Create custom framework**.

Next steps

After you create your new custom framework, you can create an assessment from your framework. For more information, see Creating an assessment in AWS Audit Manager.

To revisit your custom framework at a later date, see Finding the available frameworks in AWS Audit Manager. You can follow these steps to locate your custom framework so that you can then view, edit, share, or delete it.

Additional resources

For solutions to framework issues in Audit Manager, see Troubleshooting framework issues.

Editing a custom framework in AWS Audit Manager

You might need to modify your custom frameworks in AWS Audit Manager as your compliance requirements change.

This page outlines the steps to edit a custom framework's details and control sets.

Prerequisites

The following procedure assumes that you have previously created a custom framework.

Make sure your IAM identity has appropriate permissions to edit a custom framework in AWS Audit Manager. Two suggested policies that grant these permissions are

AWSAuditManagerAdministratorAccess and Allow users management access to AWS Audit Manager.

Procedure

Tasks

- Step 1: Edit framework details
- Step 2: Edit control sets
- Step 3. Review and save

Step 1: Edit framework details

Start by reviewing and editing the existing framework details.

To edit framework details

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the left navigation pane, choose **Framework library** and then choose the **Custom frameworks** tab.
3. Select the framework that you want to edit, choose **Actions**, and then choose **Edit**.
   - Alternatively, open a custom framework and choose **Edit** at the top right of the framework details page.
4. Under **Framework details**, review the name, compliance type, and description for your framework, and make any necessary changes.
5. Choose **Next**.

> **Tip**
>
> To edit the tags for a framework, open the framework and choose the framework tags tab. There you can view and edit the tags that are associated with the framework.

Step 2: Edit control sets

Next, review and edit the controls and control sets in the framework.

> **Note**
>
> When you use the AWS Audit Manager console to edit a custom framework, you can add up to 10 control sets for each framework.
> When you use the Audit Manager API to edit a custom framework, you can add more than 10 control sets. To add more control sets than the console currently allows, use the UpdateAssessmentFramework API that Audit Manager provides.

To edit a control set

1. Under **Control set name**, review and edit the name for your control set as needed.
2. Under **Add controls**, use the **Control type** dropdown list to select one of the two control types: **Standard controls** or **Custom controls**.
3. Based on the option you selected in the previous step, a table list of standard controls or custom controls is displayed. Select one or more controls and choose **Add to control set**.
4. In the pop-up window that appears, choose **Add**.
5. Review and edit the controls that appear in the **Selected controls** list.
   - To add more controls, repeat steps 2–4.
   - To remove unwanted controls, select one or more controls and choose **Remove from control set**.
6. To add a new control set to the framework, choose **Add control set**.
7. To remove an unwanted control set, choose **Remove control set**.
8. After you finish adding control sets and controls, choose **Next**.

Step 3. Review and save

Review the information for your framework. To change the information for a step, choose **Edit**.

When you're finished, choose **Save changes**.

Next steps

When you're certain that you no longer need a custom framework, you can clean up your Audit Manager environment by deleting the framework. For instructions, see Deleting a custom framework in AWS Audit Manager.

Additional resources

For solutions to framework issues in Audit Manager, see Troubleshooting framework issues.

Sharing a custom framework in AWS Audit Manager

You can use the framework sharing feature of AWS Audit Manager to quickly replicate the custom frameworks that you create. You can share your custom frameworks with another AWS account, or replicate your frameworks into another AWS Region under your own account. The recipient can then access your custom framework and use it to create assessments. They can do this without having to repeat any of your configuration efforts for that framework.

Key points

To share a custom framework, you create a *share request*. The recipient of the share request then has 120 days to accept or decline the request. When they accept the share request, Audit Manager replicates the shared custom framework into their framework library. In addition to replicating the custom framework, Audit Manager also replicates any custom control sets and custom controls that are part of that framework. These custom controls are then added to the recipient's control library. Audit Manager doesn't replicate standard frameworks or controls. By default, these are available in all AWS accounts and Regions where Audit Manager is enabled.

The framework sharing feature is available on the paid tier only. However, there are no additional charges for sharing a custom framework or accepting a share request. To learn more about pricing for AWS Audit Manager, see the AWS Audit Manager pricing page.

Important

You may not share a custom framework that is derived from a standard framework if the standard framework is designated as not eligible for sharing by AWS, unless you have obtained permission to do so from the owner of the standard framework. To see which standard frameworks are not eligible for sharing and learn more, see Framework sharing eligibility.

Additional resources

To learn more about how to share custom frameworks in Audit Manager, see the following resources.

- Framework sharing concepts and terminology
- Sending request to share a custom framework in AWS Audit Manager
- Responding to share requests in AWS Audit Manager
- Deleting share requests in AWS Audit Manager

Framework sharing concepts and terminology

If you learn about the following key concepts, you can get more out of the AWS Audit Manager custom framework sharing feature.

Key points

Sender

This is the creator of a share request and the AWS account where the custom framework exists. Senders can share custom frameworks with any AWS account. Or, they replicate a custom framework to any supported AWS Region under their own account.

Recipient

This is the consumer of the shared framework. Recipients can either accept or decline a share request from a sender.

> **Note**
>
> A recipient can be a delegated administrator account. However, you can't share custom frameworks with an AWS Organizations management account.

Framework eligibility

You can only share custom frameworks. By default, standard frameworks are already present in all AWS accounts and AWS Regions where AWS Audit Manager is enabled. In addition, the

custom frameworks that you share must not contain sensitive data. This includes data found within the framework itself, its control sets, and any of the custom controls that are part of the custom framework.

> **Important**
>
> Some of the standard frameworks that are offered by AWS Audit Manager contain copyrighted material that's subject to license agreements. Custom frameworks might contain content that's derived from these frameworks. You may not share a custom framework that's derived from a standard framework if the standard framework is designated as not eligible for sharing by AWS, unless you have obtained permission to do so from the owner of the standard framework.
>
> To learn which standard frameworks are eligible for sharing, refer to the following table.

Standard framework name	Custom versions eligible for sharing
Australian Cyber Security Center (ACSC) Essential Eight	 Yes
Australian Cyber Security Center (ACSC) Information Security Manual (ISM) 02 March 2023	 Yes
Amazon Web Services (AWS) Audit Manager Sample Framework	 Yes
AWS Control Tower Guardrails	 Yes
AWS generative AI Best Practices Framework v2	 Yes

Standard framework name	Custom versions eligible for sharing
AWS License Manager	 Yes
AWS Foundational Security Best Practices	 Yes
AWS Operational Best Practices	 Yes
Amazon Web Services (AWS) Well Architected Framework (WAF) v10	 Yes
Canadian Centre for Cyber Security (CCCS) Medium Cloud Control	 No
Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.2.0, Level 1	 No
Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.2.0, Level 1 and 2	 No
Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.3.0, Level 1	 No
Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.3.0, Level 1 and 2	 No

Standard framework name	Custom versions eligible for sharing
Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.4.0, Level 1	 No
Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.4.0, Level 1 and 2	 No
Center for Internet Security (CIS) v7.1, IG1	 Yes
CIS Critical Security Controls version 8.0 (CIS v8.0), IG1	 No
Federal Risk And Authorization Management Program (FedRAMP) Security Baseline Controls r4, Moderate	 Yes
General Data Protection Regulation (GDPR) 2016	 Yes
Gramm-Leach-Bliley Act (GLBA)	 Yes
Title 21 Code of Federal Regulations (CFR) Part 11, Electronic records; Electronic Signatures - Scope and Application 24 May 2023	 Yes

Standard framework name	Custom versions eligible for sharing
EudraLex - The Rules Governing Medicinal Products in the European Union (EU) - Volume 4: Good Manufacturing Practice (GMP) Medicinal Products for Human and Veterinary Use - Annex 11	Yes
Health Insurance Portability and Accountability Act (HIPAA) Security Rule: Feb 2003	Yes
Health Insurance Portability and Accountability Act (HIPAA) Omnibus Final Rule	Yes
International Organization for standardization (ISO)/International Electrotechnical Commission (IEC) 27001:2013 Annex A	No
NIST 800-53 Rev 5: Security and Privacy Controls for Information Systems and Organizations	Yes
NIST Cybersecurity Framework (CSF) v1.1	Yes
NIST 800-171 Revision 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations	Yes
Payment Card Industry Data Security Standard (PCI DSS) v3.2.1	No

Standard framework name	Custom versions eligible for sharing
Payment Card Industry Data Security Standard (PCI DSS) v4.0	 No
Statement on Standards for Attestations Engagement (SSAE) No. 18, Service Organizations Controls (SOC) Report 2	 No

Share request

To share a custom framework, you create a *share request*. The share request specifies a recipient and notifies them that a custom framework is available. Recipients have 120 days to respond to a share request by accepting or declining. If no action is taken in 120 days, the share request expires and the recipient loses the ability to add the custom framework to their framework library. Senders and recipients can view and take action on share requests from the share requests page of the framework library.

Share request status

Share requests can have any of the following statuses.

Status	Description
Active	This indicates a share request that was successfully sent to the recipient and is waiting for their response.
Expiring	This indicates a share request that expires within the next 30 days.
Shared	This indicates a share request that the recipient accepted.
Inactive	This indicates a share request that was revoked, declined, or expired before the recipient took action.
Replicating	This indicates an accepted share request that's being replicated to the recipient's framework library.

Status	Description
Failed	This indicates a share request that wasn't successfully sent to the recipient.

Share request notifications

Audit Manager notifies recipients when they receive a share request. Both recipients and senders receive a notification when a share request is due to expire sometime in the next 30 days.

- For recipients, a blue notification dot appears next to received requests with an **Active** or **Expiring** status. The recipient can resolve the notification by accepting or declining the share request.
- For senders, a blue notification dot appears next to sent requests with an **Expiring** status. The notification is resolved when the recipient accepts or declines the request. Otherwise, it's resolved when the request expires. Additionally, the sender can resolve the notification by revoking the share request.

Sender ownership

Senders maintain full access over the custom frameworks that they share. They can cancel active share requests at any time by revoking the share request before it expires. However, after a recipient accepts a share request, the sender can no longer revoke the recipient's access to that custom framework. This is because when the recipient accepts the request, Audit Manager creates an independent copy of the custom framework in the recipient's framework library.

In addition to replicating the sender's custom framework, Audit Manager also replicates any custom control sets and custom controls that are part of that framework. However, Audit Manager doesn't replicate any tags that are attached to the custom framework.

Recipient ownership

Recipients have full access over the custom frameworks that they accept. When recipient accepts the request, Audit Manager replicates the custom framework to the custom frameworks tab of their framework library. Recipients can then manage the shared custom framework in the same way as any other custom framework. Recipients can share the custom frameworks that they receive from other senders. Recipients can't block senders from sending share requests.

Shared framework expiration

When a sender creates a share request, Audit Manager sets the request to expire after 120 days. Recipients can accept and gain access to the shared framework before the request expires. If a recipient doesn't accept during this time, the share request expires. After this point, a record of the expired share request remains in their history. Snapshots of expired shared frameworks are archived to an S3 bucket with a one-year TTL for audit purposes.

Senders can choose to revoke a share request at any time before it's due to expire.

Shared framework data storage and backup

When you create a share request, Audit Manager stores a snapshot of your custom framework in the US East (N. Virginia) AWS Region. Audit Manager also stores a backup of the same snapshot in the US West (Oregon) AWS Region.

Audit Manager deletes the snapshot and the backup snapshot when one of the following events occurs:

- The sender revokes the share request.
- The recipient declines the share request.
- The recipient encounters an error and doesn't successfully accept the share request.
- The share request expires before the recipient responds to the request.

When a sender resends a share request, the snapshot is replaced with an updated version that corresponds with the latest version of the custom framework.

When a recipient accepts a share request, the snapshot is replicated into their AWS account under the AWS Region that was specified in the share request.

Shared framework versioning

When you share a custom framework, Audit Manager creates an independent copy of that framework in the specified AWS account and Region. This means that you should keep in mind the following points:

- The shared framework that a recipient accepts is a snapshot of the framework at the time of the share request creation. If you update the original custom framework after sending a share request, the request isn't automatically updated. To share the latest version of the updated framework, you can resend the share request. The expiration date of this new snapshot is 120 days from the re-share date.

- When you share a custom framework with another AWS account and then delete it from your framework library, the shared custom framework remains in the recipient's framework library.
- When you share a custom framework to another AWS Region under your account and then delete that custom framework in the first AWS Region, the custom framework remains in the second Region.
- When you delete a shared custom framework after accepting it, any custom controls that were replicated as part of the custom framework remain in your control library.

Additional resources

- Sending request to share a custom framework in AWS Audit Manager
- Responding to share requests in AWS Audit Manager
- Deleting share requests in AWS Audit Manager
- Troubleshooting framework issues

Sending request to share a custom framework in AWS Audit Manager

This tutorial describes how to share your custom frameworks across AWS accounts and AWS Regions.

When you share a custom framework, Audit Manager creates a snapshot of your framework and sends a share request to the recipient. The recipient has 120 days to accept the shared framework. When they accept, Audit Manager replicates the shared custom framework to their framework library in the specified AWS Region. If you want to replicate a custom framework to another Region under your own account, use the following tutorial and enter your own AWS account ID as the recipient account ID.

Prerequisites

Before you start this tutorial, make sure that you first meet the following conditions:

- You're familiar with Audit Manager framework sharing concepts and terminology.
- The custom framework that you want to share is eligible for sharing and exists in the framework library of your AWS Audit Manager environment.
- The recipient already enabled AWS Audit Manager in the AWS Region where you want to share the custom framework.

- The recipient is not an AWS Organizations management account.
- Your IAM identity has appropriate permissions to share a custom framework in AWS Audit Manager. Two suggested policies that grant these permissions are AWSAuditManagerAdministratorAccess and Allow users management access to AWS Audit Manager.

> **Tip**
>
> Before you start, make a note of the AWS account ID that you want to share your custom framework with. This can be your own account ID, if your goal is to replicate the framework to another AWS Region under your account. You need this information for step 2 of the tutorial.

Procedure

Tasks

- Step 1: Identify the custom framework that you want to share
- Step 2: Send a share request
- Step 3: View your sent requests
- Step 4 (Optional): Revoke the share request

Step 1: Identify the custom framework that you want to share

Start by identifying the custom framework that you want to share. You can find a list of all available custom frameworks on the **Framework library** page in Audit Manager.

> **Important**
>
> Don't share custom frameworks that contain sensitive data. This includes data found within the framework itself, its control sets, and any of the custom controls that comprise the custom framework. For more information, see Framework eligibility.

To view your available custom frameworks

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the navigation pane, choose **Framework library**.
3. Choose the **Custom frameworks** tab. This displays a list of your available custom frameworks. You can choose any framework name to view the details of that custom framework.

Step 2: Send a share request

Next, specify a recipient and send them a share request for the custom framework. The recipient has 120 days to respond to the share request before it expires.

To send a share request

1. From the **Custom frameworks** tab of the framework library, choose the name of a framework to open the detail page. From here, choose **Actions** and then choose **Share custom framework**.
   - Alternatively, select a custom framework from the list in the framework library, choose **Actions**, and then choose **Share custom framework**. Depending on the size of the custom framework, this method can take a few seconds while Audit Manager prepares the share request.
2. Review the notice that displays in the dialog box.
   - If you're unsure whether you can share your custom framework, review Framework eligibility for further guidance.
   - If your framework has controls that use custom AWS Config rules as a data source, we recommend that you contact the recipient to let them know. The recipient can then create and enable the same AWS Config rules in their instance of AWS Config. For more information, see My shared framework has controls that use custom AWS Config rules as a data source. Can the recipient collect evidence for these controls?.
3. Enter **`agree`** and then choose **Agree** to proceed.
4. On the next screen, follow these steps:
   - Under **AWS account**, enter the recipient's account ID. This can be your own account ID.
   - Under **AWS Region**, select the recipient's Region from the dropdown list.

- (Optional) Under **Message to recipient**, enter an optional comment about the custom framework that you're sharing.
- Under **Custom framework details**, review the details to confirm that you want to share this framework.

5. Choose **Share**.

> **Note**
>
> Keep in mind the following points:
>
> - When you share a custom framework with another AWS account, the framework is replicated only to the specified AWS Region. After accepting the share request, the recipient can then replicate the framework across Regions as needed.
> - When sharing custom frameworks across AWS Regions, it can take up to 10 minutes to process share request actions. After sending a cross-Region share request, we recommend that you check back later to confirm that your share request was sent successfully.
> - When you send a share request, Audit Manager takes a snapshot of the custom framework at the time of the share request creation. If you update the custom framework after sending a share request, the request isn't automatically updated. To share the latest version of an updated framework, you can resend the share request. The expiration date of this new snapshot is 120 days from the re-share date.

Step 3: View your sent requests

You can select the **Sent requests** tab to see a list of all the share requests that you sent. You can filter this list as needed. For example, you can apply filters to display only requests that expire within the next 30 days.

To view and filter your sent requests

1. From the navigation pane, choose **Share requests**.
2. Choose the **Sent requests** tab.
3. (Optional) Apply filters to fine-tune which sent requests are visible. You can do this by finding the **All statuses** dropdown list, and changing the filter to one of the following.

Status	Description
Active	This filter displays share requests that are awaiting a response from the recipient.
Expiring	This filter displays share requests that expire in the next 30 days.
Shared	This filter displays share requests that were accepted by the recipient. The shared custom framework now exists in the recipient's framework library.
Inactive	This filter displays share requests that were declined, revoked, or expired before the recipient took action. Choose the word **Inactive** to view more details.
Replicating	This indicates an accepted share request that's being replicated to the recipient's framework library.
Failed	This filter displays the share requests that weren't successfu lly sent to the recipient. Choose the word **Failed** to view more details.

Note

It can take up to 15 minutes to process a share request. As a result, if an error occurred when sending your share request to the recipient, the *Failed* status might not display immediately. We recommend that you check back later to confirm that your share request was sent successfully.

Step 4 (Optional): Revoke the share request

If you need to cancel an active share request before it's due to expire, you can revoke the request at any time. This step is optional. If you take no action, the recipient loses the ability to accept the share request after the expiration date.

To revoke a share request

1. From the navigation pane, choose **Share requests**.
2. Choose the **Sent requests** tab.
3. Select the framework that you want to revoke and choose **Revoke request**.
4. In the pop-up window that appears, choose **Revoke**.

> **Note**
>
> You can only revoke access to share requests that have a status of *Active* or *Expiring*. After a recipient accepts a share request, you can no longer revoke their access to that custom framework. This is because a copy of the custom framework now exists in the recipient's framework library.
>
> When sharing frameworks across AWS Regions, it can take up to 10 minutes to process share request actions. After revoking a cross-Region share request, we recommend that you check back later to confirm that the share request was revoked successfully.

Next steps

Resending a share request for an updated framework

You might send a share request for a custom framework and then update the same framework afterwards. If you do this, the share request isn't automatically updated to reflect the latest version of the framework. However, if its status is *active*, *shared*, or *expiring*, you can update an existing share request. To do this, you resend a new share request with the same set of details as the existing request. In the new share request, include the same custom framework ID, recipient account ID, and recipient AWS Region. You can also provide a new comment with the new share request.

Keep in mind the following when you resend a share request:

- For the update to be successful, the new request must be for the same custom framework ID. It must also specify the same recipient account ID and Region as the existing request.
- If the name of the custom framework has changed, the updated share request displays the latest name.
- If you provide a new comment, the updated share request displays the latest comment.

- When you resend a share request, the expiration date is extended by six months.

To resend a share request for an updated framework

1. From the **Custom frameworks** tab of the framework library, choose the name of the framework that you want to share. This opens the framework detail page.
2. Choose **Actions** and then choose **Share custom framework**.
3. Review the notice that displays in the dialog box, enter **`agree`**, and then choose **Agree** to proceed.
4. On the next screen, follow these steps:
   - Under **AWS account**, enter the same account ID that you specified in the existing share request.
   - Under **AWS Region**, select the same Region that you specified in the existing share request.
   - (Optional) Under **Message to recipient**, enter an optional comment about the updated custom framework.
   - Under **Custom framework details**, review the details to confirm that you want to resend the share request.
5. Choose **Share** to resend and update the share request.

Additional resources

To find solutions to the issues that you might encounter when sharing a custom framework, see Troubleshooting framework issues.

Responding to share requests in AWS Audit Manager

This tutorial describes the actions to take when you receive a share request for a custom framework. Audit Manager notifies you when you receive a share request. You also receive a notification to remind you when a share request is due to expire in the next 30 days.

Prerequisites

Before you get started, we recommend that you first learn more about Audit Manager framework sharing concepts and terminology.

Procedure

Tasks

- Step 1: Check your received request notifications
- Step 2: Take action on the request
- Step 3: View a history of your received requests

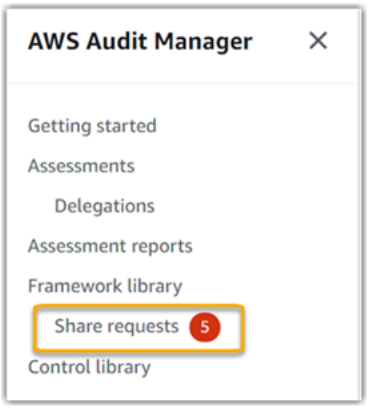
Step 1: Check your received request notifications

Start by checking your share request notifications. The **Received requests** tab displays a list of the share requests that you've received from other AWS accounts. Requests that are awaiting your response appear with a blue dot. You can also filter this view to display only requests that expire sometime within the next 30 days.

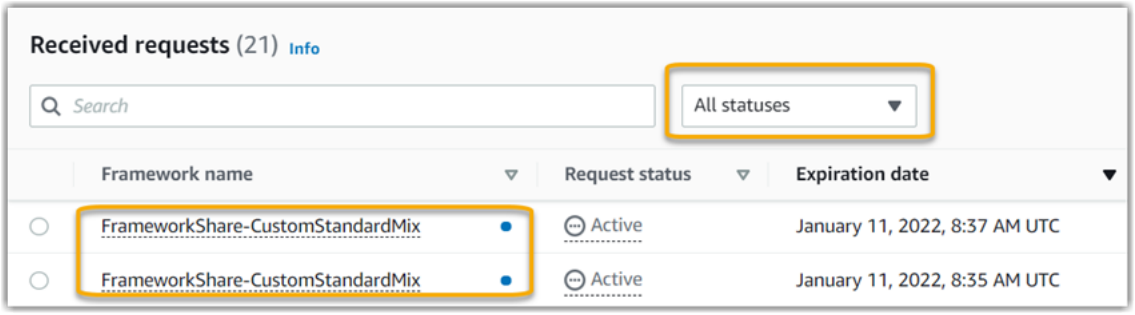
To view received requests

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. If you have a share request notification, Audit Manager displays a red dot next to the navigation menu icon.

3. Expand the navigation pane and look next to **Share requests**. A notification badge indicates the number of share requests that need your attention.



4. Choose **Share requests**. By default, this page opens on the **Received requests** tab.
5. Identify the share requests that need your action by looking for items with a blue dot.



6. (Optional) To view only requests that expire in the next 30 days, find the **All statuses** dropdown list and select **Expiring**.

Step 2: Take action on the request

To remove the blue notification dot, you need to take action by either accepting or declining the share request.

Accepting a shared framework

When you accept a share request, Audit Manager replicates a snapshot of the original framework into the custom frameworks tab of your framework library. Audit Manager replicates and encrypts the new custom framework using the KMS key that you specified in your Audit Manager settings.

To accept a share request

1. Open the **Share requests** page and make sure that you're viewing the **Received requests** tab.
2. (Optional) Select **Active** or **Expiring** from the filter dropdown list.
3. (Optional) Choose a framework name to view the details of the share request. This includes information such as the framework description, the number of controls that are in the framework, and the message from the sender.
4. Select the share request that you want to accept, choose **Actions**, and then choose **Accept**.

After you accept a share request, the status changes to *replicating* while the shared custom framework is added to your framework library. If the framework contains custom controls, these controls are added to your control library at this time.

When the framework replication is complete, the status changes to *shared*. A success banner notifies you that the custom framework is ready to use.

> **Tip**
>
> When you accept a custom framework, it's replicated only to your current AWS Region. You might want the new shared framework to be available across all Regions in your AWS account. If so, after you accept the share request you can share the framework to other Regions under your account as needed.

Declining a shared framework

When you decline a share request, Audit Manager doesn't add that custom framework to your framework library. However, a record of the declined share request remains in the **Received requests** tab, with a status of **Inactive**.

To decline a share request

1. Open the **Share requests** page and make sure that you're viewing the **Received requests** tab.
2. (Optional) Select **Active** or **Expiring** from the filter dropdown list.
3. (Optional) Choose a framework name to view the details of the share request. This includes information such as the framework description, the number of controls that are in the framework, and the message from the sender.
4. Select the share request that you want to decline, choose **Actions**, and then choose **Decline**.
5. In the dialog box that appears, choose **Decline** to confirm your choice.

> **Tip**
>
> If you change your mind and want access to a shared framework after you decline, ask the sender to send you a new share request.

> **Note**
>
> It can take up to 10 minutes to process share request actions when a framework is shared across AWS Regions. After taking action on a cross-Region share request, we recommend that you check back later to confirm that the share request was successfully accepted or declined.

Step 3: View a history of your received requests

After you accept or decline a shared framework, you can return to the **Share requests** page to see your share request history. You can filter this list as needed. For example, you can apply filters to display only requests that you accepted.

To view a history of your share requests

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the left navigation pane, choose **Share requests**.
3. Choose the **Received requests** tab.
4. Find the **All statuses** dropdown list, and select one of the following filters:

Name	Description
Active	This filter displays share requests that you haven't yet accepted or declined.
Expiring	This filter displays share requests that expire in the next 30 days.
Shared	This filter displays share requests that you accepted. The shared framework is now available in your framework library.
Inactive	This filter displays share requests that were declined or expired.
Failed	This filter displays the share requests that weren't sent successfully. Choose the word **Failed** to view more details.

Next steps

After you accept a shared custom framework, you can find it in the custom frameworks tab of the framework library. You can now use that framework to create an assessment. To learn more, see Creating an assessment in AWS Audit Manager.

For instructions on how to edit your new custom framework, see Editing a custom framework in AWS Audit Manager.

Additional resources

To find solutions to issues that you might encounter, see Troubleshooting framework issues.

Deleting share requests in AWS Audit Manager

When you no longer need a share request, you can delete it from your Audit Manager environment. This enables you to clean up your workspace and focus on the requests that are relevant to your current tasks and priorities.

When you delete a share request, only the request itself is deleted. The shared framework itself remains in your framework library.

Prerequisites

The following procedure assumes that you have previously sent or received a share request. You can't delete share requests that have a status of *active* or *replicating*.

Make sure your IAM identity has appropriate permissions to delete a share request in AWS Audit Manager. Two suggested policies that grant these permissions are AWSAuditManagerAdministratorAccess and Allow users management access to AWS Audit Manager.

Procedure

To delete a share request

1. From the navigation pane, choose **Share requests**.
2. Choose either the **Sent requests** or the **Received requests** tab.
3. Select the framework that you no longer want and choose **Delete**.
4. In the pop-up window that appears, choose **Delete**.

Additional resources

To find solutions to issues that you might encounter, see Troubleshooting framework issues.

Deleting a custom framework in AWS Audit Manager

When you no longer need a custom framework, you can delete it from your Audit Manager environment. This enables you to clean up your workspace and focus on the custom frameworks that are relevant to your current tasks and priorities.

Prerequisites

The following procedure assumes that you have previously created a custom framework.

Make sure your IAM identity has appropriate permissions to delete a custom framework in AWS Audit Manager. Two suggested policies that grant these permissions are AWSAuditManagerAdministratorAccess and Allow users management access to AWS Audit Manager.

Procedure

You can delete custom frameworks using the Audit Manager console, the Audit Manager API, or the AWS Command Line Interface (AWS CLI).

> **Note**
>
> Deleting a custom framework doesn't affect any existing assessments that were created from the framework before it was deleted.

Audit Manager console

To delete a custom framework on the Audit Manager console

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the left navigation pane, choose **Framework library** and then choose the **Custom frameworks** tab.
3. Select the framework that you want to delete, choose **Actions**, and then choose **Delete**.
   - Alternatively, you can open a custom framework and choose **Actions**, **Delete** at the top right of the framework summary page.
4. In the pop-up window, choose **Delete** to confirm deletion.

AWS CLI

To delete a custom framework in the AWS CLI

1. First, identify the custom framework that you want to delete. To do this, run the list-assessment-frameworks command and specify the `--framework-type` as `Custom`.

   ```
   aws auditmanager list-assessment-frameworks --framework-type Custom
   ```

   The response returns a list of custom frameworks. Find the custom framework that you want to delete, and take note of the framework ID.
2. Next, run the delete-assessment-framework command and specify the `--framework-id` of the framework that you want to delete.

   In the following example, replace the *`placeholder text`* with your own information.

   ```
   aws auditmanager delete-assessment-framework --framework-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

Audit Manager API

To delete a custom framework using the API

1. Use the ListAssessmentFrameworks operation and specify the frameworkType as `Custom`. From the response, find the custom framework that you want to delete, and take note of the framework ID.
2. Use the DeleteAssessmentFramework operation to delete the framework. In the request, use the frameworkId parameter to specify the framework that you want to delete.

For more information about these API operations, choose any of the links in the previous procedure to read more in the *AWS Audit Manager API Reference*. This includes information about how to use these operations and parameters in one of the language-specific AWS SDKs.

Additional resources

For information about data retention in Audit Manager, see Deletion of Audit Manager data.

Using the control library to manage controls in AWS Audit Manager

You can access and manage controls from the control library in AWS Audit Manager.

Key points

In the control library, controls are organized into the following categories.

- **Common controls** collect evidence that supports multiple overlapping compliance standards. Automated common controls contain one or more related core controls that each collect supporting evidence from a predefined group of data sources. This provides you with an efficient way to identify the AWS data sources that map to your portfolio of compliance requirements. The underlying data sources for each automated common control are validated and maintained by industry certified assessors in AWS Security Assurance Services.
- **Standard controls** collect evidence to support a specific compliance standard. You can view the details of standard controls, but you can't edit or delete them. However, you can make an editable copy of any standard control to create a new control that meets your specific requirements.
- **Custom controls** are controls that you own and define. When you create a custom control, we recommend that you choose the common controls that represent your goals and use them as an evidence source. As a result, your custom control can collect all of the evidence that's relevant to those common controls. You can also use core controls as an evidence source, or use other sources that you define yourself. When you're done, add your custom controls to a custom framework, and then create an assessment to start collecting evidence.

Additional resources

To create and manage controls in Audit Manager, follow the procedures that are outlined here.

- Finding the available controls in AWS Audit Manager
- Reviewing a control in AWS Audit Manager
  - Reviewing a common control
  - Reviewing a core control

Finding the available controls in AWS Audit Manager

You can find all available controls on the **Control library** page in the Audit Manager console.

You can also view all available controls using the Audit Manager API or the AWS Command Line Interface (AWS CLI).

Prerequisites

Make sure your IAM identity has appropriate permissions to view controls in AWS Audit Manager. Two suggested policies that grant these permissions are AWSAuditManagerAdministratorAccess and Allow users management access to AWS Audit Manager.

Procedure

Audit Manager console

To view available controls on the Audit Manager console

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.

2. In the navigation pane, choose **Control library**.
3. Choose a tab to browse the available controls.

   - Choose **Common** to see the common controls that are provided by AWS.
   - Choose **Standard** to see the standard controls that are provided by AWS.
   - Choose **Custom** to see the custom controls that you created.

AWS CLI

To find common controls in the (AWS CLI

Run the list-common-controls command to see a list of common controls.

```
aws controlcatalog list-common-controls
```

You can also use the optional `common-control-filter` attribute to return a list of common controls that have a specific objective.

In the following example, replace the *`placeholder text`* with your own information.

```
aws controlcatalog list-common-controls --common-control-filter OBJECTIVE-ARN
```

To find other types of controls in the AWS CLI

Run the list-controls command and specify the `--control-type` as `Custom`, `Standard`, or `Core`.

In the following example, replace the *`placeholder text`* with your own information.

```
aws auditmanager list-controls --control-type Type
```

Audit Manager API

To find common controls using the API

Use the ListCommonControls operation to see a list of available common controls. You can also use the optional `commonControlFilter` attribute to return a list of controls that have a specific objective.

To find other types of control using the API

Use the ListControls operation and specify the controlType as `Custom`, `Standard`, or `Core`.

For more information, choose any of the links in the previous procedure to read more in the *AWS Audit Manager API Reference*. This includes information about how to use these operations and parameters in one of the language-specific AWS SDKs.

Next steps

When you're ready to explore the details of a control, follow the steps in Reviewing a control in AWS Audit Manager. This page will guide you through the control details and explain the information that you see there.

From the control library page, you can also create a custom control, edit a custom control, or delete a custom control.

Additional resources

For solutions to control issues in Audit Manager see Troubleshooting control and control set issues.

Reviewing a control in AWS Audit Manager

You can review the details of a control by using the Audit Manager console, the Audit Manager API, or the AWS Command Line Interface (AWS CLI).

To get started with reviewing a control in Audit Manager, follow the procedures that are outlined here.

- Reviewing a common control
- Reviewing a core control
- Reviewing a standard control
- Reviewing a custom control

Reviewing a common control

When you need to review the details of a control, you'll find the information organized into several sections on the control details page. These sections help you easily access and understand the relevant information for that control.

Prerequisites

Make sure your IAM identity has appropriate permissions to view common controls in Audit Manager. More specifically, you need the following permissions to view the common controls, control objectives, and control domains that are provided by AWS Control Catalog:

- `controlcatalog:ListCommonControls`
- `controlcatalog:ListDomains`
- `controlcatalog:ListObjectives`

A suggested policy that grants these permissions is AWSAuditManagerAdministratorAccess.

Procedure

You can review a common control using the Audit Manager console, the AWS Control Catalog API, or the AWS Command Line Interface (AWS CLI).

Audit Manager console

To view common control details on the Audit Manager console

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the navigation pane, choose **Control library**.
3. Choose **Common** to see the common controls that are provided by AWS.
4. Choose any common control name to view the details for that control.
5. Review the common control details using the following information as reference.

Overview section

This section describes the common control.

Evidence sources tab

This tab includes the following information:

Name	Description
Core controls	These are the core controls that collect evidence to support the common control. • When you collect evidence for this common control, you automatically collect evidence for all of the core controls that are listed here. When each of these core controls is implemented successfully, this helps to demonstrate that you're meeting the requirements of the common control. • Each core control uses a predefined grouping of data sources to collect evidence about an AWS service. AWS manages these data sources for you. This means that they're automatically updated whenever regulations and standards change and new data sources are identifie d. Choose any core control to see the underlying data sources.

Related requirements tab

When you collect evidence for this common control, the same evidence can help you to demonstrate compliance with the requirements of the related standard controls that are listed on this tab. Choose any standard control to see more details.

> **Note**
>
> - The common control might produce evidence that demonstrates only partial compliance with a standard control. It's possible that you might need additional evidence to demonstrate full compliance with a standard control.
> - At this time, the **Related requirements** tab shows related standard controls only. Although a common control can be related to one or more custom controls, those relationships aren't displayed in this tab.

AWS CLI

To view common control details in the AWS CLI

1. Run the list-common-controls command to see a list of available common controls. When you use this operation, you can apply an optional `common-control-filter` to see common controls that have a specific objective.

```
aws controlcatalog list-common-controls
```

2. In the response, identify the common control that you want to review and take note of its details.

AWS Control Catalog API

To view common control details using the API

1. Use the ListCommonControls operation to see a list of available common controls. When you use this operation, you can apply an optional `commonControlFilter` to see a list of controls that have a specific objective.
2. In the response, identify the control that you want to review and take note of its details.

For more information about these API operations, choose the link in this procedure to read more in the *AWS Control Catalog API Reference*. This includes information about how to use these operations and parameters in one of the language-specific AWS SDKs.

Next steps

You can choose the common controls that represent your goals and use them as building blocks to create a custom control. Each automated common control maps to a predefined grouping of AWS data sources that Audit Manager handles for you. This means that you don’t have to be an AWS expert to know which data sources collect the relevant evidence for your goals. Moreover, you don't have to maintain these data source mappings yourself.

For instructions on how to create a custom control that uses common controls as an evidence source, see Creating a custom control in AWS Audit Manager.

Additional resources

- Reviewing a core control
- Reviewing a standard control
- Reviewing a custom control

Reviewing a core control

You can review the details of a core control by using the Audit Manager console, the Audit Manager API, or the AWS Command Line Interface (AWS CLI).

Prerequisites

Make sure your IAM identity has appropriate permissions to view controls in AWS Audit Manager. Two suggested policies that grant these permissions are AWSAuditManagerAdministratorAccess and Allow users management access to AWS Audit Manager.

Procedure

Audit Manager console

To view core control details on the Audit Manager console

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the navigation pane, choose **Control library**.
3. Choose **Common** to see the common controls that are provided by AWS.
4. Look for the common control that meets your use case.
5. Choose the tree view icon next to the common control name. This displays the core controls that support the common control.
6. Choose the name of the core control that you want to review.
7. Review the core control details using the following information as reference.

Overview section

This section describes the core control and lists the data source types where it collects evidence from.

Evidence sources tab

This tab includes the following information:

Name	Description

Data sources	These are the AWS managed data sources that the core control collects evidence from. These data sources are automatically updated whenever regulations and standards change and new data sources are identified.
	• **Mapping** – The specific keyword that's used to collect evidence.
	  • If the type is *AWS Config*, the mapping is an AWS Config rule (such as `SNS_ENCRYPTED_KMS`).
	  • If the type is *AWS Security Hub*, the mapping is a Security Hub control (such as `EC2.1`).
	  • If the type is *AWS API calls*, the mapping is an API call (such as `kms_ListKeys`).
	  • If the type is *AWS CloudTrail*, the mapping is a CloudTrail event (such as `CreateAccessKey`).
	• **Type** – The type of data source that the evidence comes from.
	  • If Audit Manager collects the evidence, the type can be *AWS Security Hub*, *AWS Config*, *AWS CloudTrail*, or *AWS API calls*.
	  • If you upload your own evidence, the type is *Manual*. A description indicates if the required manual evidence is a *File upload* or a *Text response*.
	• **Frequency** – How often Audit Manager collects evidence for an AWS API call data source.

Details tab

This tab includes the following information:

Name	Description
Instructions	The directions that describe how to test and remediate the control.
Testing information	The recommended testing procedures.
Action plan	The recommended actions to take if you need to remediate the control.

AWS CLI

To view core control details in the AWS CLI

1. Follow the steps to find a control. Make sure to set the `--control-type` as `Core`, and apply any optional filters as needed.

```
aws auditmanager list-controls --control-type Core
```

2. In the response, identify the control that you want to review and take note of the control ID and Amazon Resource Name (ARN).
3. Run the get-control command and specify the `--control-id`. In the following example, replace the *`placeholder text`* with your own information.

```
aws auditmanager get-control --control-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

> **Tip**
>
> The control details are returned in JSON format. To help you understand this data, see get-control Output in the *AWS CLI Command Reference*.

4. To see tag details, run the list-tags-for-resource command and specify the `--resource-arn`. In the following example, replace the *`placeholder text`* with your own information.

```
aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:control/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Audit Manager API

To view core control details using the API

1. Follow the steps to find a control. Make sure to set the controlType as `Core`, and apply any optional filters as needed.
2. In the response, identify the control that you want to review and take note of the control ID and Amazon Resource Name (ARN).
3. Use the GetControl operation and specify the controlId that you noted in step 2.

   > **Tip**
   >
   > The control details are returned in JSON format. To help you understand this data, see GetControl Response Elements in the *AWS Audit Manager API Reference*.

4. To see tag details, use the ListTagsForResource operation and specify the resourceArn that you noted in step 2.

For more information about these API operations, choose any of the links in this procedure to read more in the *AWS Audit Manager API Reference*. This includes information about how to use these operations and parameters in one of the language-specific AWS SDKs.

Next steps

You can choose the core controls that represent your goals and use them as building blocks to create a custom control. Each automated core control maps to a predefined grouping of AWS data sources that Audit Manager handles for you. This means that you don't have to be an AWS expert to know which data sources collect the relevant evidence for your goals. Moreover, you don't have to maintain these data source mappings yourself.

For instructions on how to create a custom control that uses core controls as an evidence source, see Creating a custom control in AWS Audit Manager.

Additional resources

- Reviewing a common control
- Reviewing a standard control

- Reviewing a custom control

Reviewing a standard control

You can review the details of a standard control by using the Audit Manager console, the Audit Manager API, or the AWS Command Line Interface (AWS CLI).

Prerequisites

Make sure your IAM identity has appropriate permissions to view controls in AWS Audit Manager. Two suggested policies that grant these permissions are AWSAuditManagerAdministratorAccess and Allow users management access to AWS Audit Manager.

Procedure

You can review the details of a standard control by using the Audit Manager console, the Audit Manager API, or the AWS Command Line Interface (AWS CLI).

Audit Manager console

To view standard control details on the Audit Manager console

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the navigation pane, choose **Control library**.
3. Choose **Standard** to see the standard controls that are provided by AWS.
4. Choose any standard control name to view the details for that control.
5. Review the standard control details using the following information as reference.

Overview section

This section describes the standard control and lists the data source types that it uses to collect evidence.

Evidence sources tab

This tab includes the following information:

Name	Description
Core controls	These are the core controls that collect evidence to support the standard control. Each core control uses a predefined grouping of data sources to collect evidence about an AWS service. These data sources are managed for you by AWS, and are automatically updated whenever regulations and standards change and new data sources are identified. Choose any core control to see the underlying data sources.

Data sources	These are the other AWS managed data sources that collect evidence to support the standard control.
	• **Mapping** – The specific keyword that's used to collect evidence.
	  • If the type is *AWS Config*, the mapping is an AWS Config rule (such as `SNS_ENCRYPTED_KMS`).
	  • If the type is *AWS Security Hub*, the mapping is a Security Hub control (such as `EC2.1`).
	  • If the type is *AWS API calls*, the mapping is an API call (such as `kms_ListKeys`).
	  • If the type is *AWS CloudTrail*, the mapping is a CloudTrail event (such as `CreateAccessKey`).
	• **Type** – The type of data source that the evidence comes from.
	  • If Audit Manager collects the evidence, the type can be *AWS Security Hub*, *AWS Config*, *AWS CloudTrail*, or *AWS API calls*.
	  • If you upload your own evidence, the type is *Manual*. A description indicates if the required manual evidence is a *File upload* or a *Text response*.
	• **Frequency** – How often Audit Manager collects evidence for an AWS API call data source.

Details tab

This tab includes the following information:

Name	Description
Instructions	The directions that describe how to test and remediate the control.
Testing information	The recommended testing procedures.
Action plan	The recommended actions to take if you need to remediate the control.
Tags	The tags that are associated with the control.
Key	The tag key (for example, a compliance standard, regulation, or category).
Value	The tag value.

AWS CLI

To view standard control details in the AWS CLI

1. Follow the steps to find a control. Make sure to set the `--control-type` as `Standard`, and apply any optional filters as needed.

```
aws auditmanager list-controls --control-type Standard
```

2. In the response, identify the control that you want to review and take note of the control ID and Amazon Resource Name (ARN).
3. Run the get-control command and specify the `--control-id`. In the following example, replace the *placeholder text* with your own information.

```
aws auditmanager get-control --control-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

> **Tip**
>
> The control details are returned in JSON format. To help you understand this data, see get-control Output in the *AWS CLI Command Reference*

4. To see tag details, run the list-tags-for-resource command and specify the `--resource-arn`. In the following example, replace the *`placeholder text`* with your own information.

```
aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:control/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Audit Manager API

To view standard control details using the API

1. Follow the steps to find a control. Make sure to set the controlType as `Standard`, and apply any optional filters as needed.
2. In the response, identify the control that you want to review and take note of the control ID and Amazon Resource Name (ARN).
3. Use the GetControl operation and specify the controlId that you noted in step 2.

> **Tip**
>
> The control details are returned in JSON format. To help you understand this data, see GetControl Response Elements in the *AWS Audit Manager API Reference*.

4. To see tag details, use the ListTagsForResource operation and specify the resourceArn that you noted in step 2.

For more information about these API operations, choose any of the links in this procedure to read more in the *AWS Audit Manager API Reference*. This includes information about how to use these operations and parameters in one of the language-specific AWS SDKs.

Next steps

You can add a standard control to any of your custom frameworks. For instructions, see Creating a custom framework in AWS Audit Manager.

You can also customize any standard control so that it meets your needs. For instructions, see Making an editable copy of a control in AWS Audit Manager.

Additional resources

- Reviewing a common control
- Reviewing a core control
- Reviewing a custom control

Reviewing a custom control

You can review the details of a custom control by using the Audit Manager console, the Audit Manager API, or the AWS Command Line Interface (AWS CLI).

Prerequisites

Make sure your IAM identity has appropriate permissions to view controls in AWS Audit Manager. Two suggested policies that grant these permissions are AWSAuditManagerAdministratorAccess and Allow users management access to AWS Audit Manager.

Procedure

You can review the details of a custom control by using the Audit Manager console, the Audit Manager API, or the AWS Command Line Interface (AWS CLI).

Audit Manager console

To view custom control details on the Audit Manager console

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the navigation pane, choose **Control library**.
3. Choose **Custom** to see the custom controls that you created.
4. Choose any custom control name to view the details for that control.

5. Review the custom control details using the following information as reference.

Overview section

This section describes the custom control and lists the data source types that it uses to collect evidence. It also provides information about when the control was created and last updated.

Evidence sources tab

This tab shows where the custom control collects evidence from. It includes the following information:

Name	Description
Common controls	These are the common controls that collect evidence to support the custom control. Common controls collect evidence using underlying data sources that AWS manages for you. For every common control that's listed, Audit Manager collects the relevant evidence for all of the supporting core controls. Choose a common control to see the related core controls.
Core controls	These are the core controls that collect evidence to support the custom control. Core controls collect evidence by using a predefined group of data sources that AWS manages for you. Choose a core control to see the underlying data sources.
Data sources	These are the data sources that collect evidence to support the custom control. **Note** These data sources aren't managed for you by AWS. You're responsible for maintaining them.

Name	Description

	• **Name** – The name of the data source.
	• **Type** – The type of data source that the evidence comes from.
	  • If Audit Manager collects the evidence, the type can be *AWS Security Hub*, *AWS Config*, *AWS CloudTrail*, or *AWS API calls*.
	  • If you upload your own evidence, the type is *Manual*. A description indicates if the required manual evidence is a *File upload* or a *Text response*.
	• **Mapping** – The specific keyword that's used to collect evidence.
	  • If the type is *AWS Config*, the mapping is an AWS Config rule (such as `SNS_ENCRYPTED_KMS`).
	  • If the type is *AWS Security Hub*, the mapping is a Security Hub control (such as `EC2.1`).
	  • If the type is *AWS API calls*, the mapping is an API call (such as `kms_ListKeys`).
	  • If the type is *AWS CloudTrail*, the mapping is a CloudTrail event (such as `CreateAccessKey`).
	• **Frequency** – How often Audit Manager collects evidence for an AWS API call data source.

Details tab

This tab includes the following information:

Name	Description
Instructions	The directions that describe how to test and remediate the control.
Testing information	The recommended testing procedures.

Name	Description
Action plan	The recommended actions to take if you need to remediate the control.
Tags	The tags that are associated with the control.
Key	The tag key (for example, a compliance standard, regulation, or category).
Value	The tag value.

AWS CLI

To view custom control details in the AWS CLI

1. Follow the steps to find a control. Make sure to set the `--control-type` as `Custom`, and apply any optional filters as needed.

```
aws auditmanager list-controls --control-type Custom
```

2. In the response, identify the control that you want to review and take note of the control ID and Amazon Resource Name (ARN).
3. Run the get-control command and specify the `--control-id`. In the following example, replace the *`placeholder text`* with your own information.

```
aws auditmanager get-control --control-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

> **Tip**
>
> The control details are returned in JSON format. To help you understand this data, see get-control Output in the *AWS CLI Command Reference*.

4. To see the tags for a control, use the list-tags-for-resource command and specify the `--resource-arn`. In the following example, replace the *`placeholder text`* with your own information:

```
aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:control/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Audit Manager API

To view custom control details using the API

1. Follow the steps to find a control. Make sure to set the controlType as `Custom`, and apply any optional filters as needed.
2. In the response, identify the control that you want to review and take note of the control ID and its Amazon Resource Name (ARN).
3. Use the GetControl operation and specify the controlId that you noted in step 2.

   > **Tip**
   >
   > The control details are returned in JSON format. To help you understand this data, see GetControl Response Elements in the *AWS Audit Manager API Reference*.

4. To see tags for the control, use the ListTagsForResource operation and specify the control resourceArn that you noted in step 2.

For more information about these API operations, choose any of the links in this procedure to read more in the *AWS Audit Manager API Reference*. This includes information about how to use these operations and parameters in one of the language-specific AWS SDKs.

Next steps

You can add a custom control to any of your custom frameworks. For instructions, see Creating a custom framework in AWS Audit Manager.

You can also edit a custom control, make an editable copy of a custom control, or delete a custom control that you no longer need.

Additional resources

- Reviewing a common control

- Reviewing a core control
- Reviewing a standard control

Creating a custom control in AWS Audit Manager

You can use custom controls to collect evidence for your specific compliance needs.

Just like standard controls, custom controls collect evidence continually when they're active in your assessments. You can also add manual evidence to any custom control that you create. Each piece of evidence becomes a record that helps you to demonstrate compliance with your custom control's requirements.

To get started, here are some examples of how you can use custom controls:

Map your enterprise controls to predefined groupings of AWS data sources

You can onboard your enterprise controls to Audit Manager by using common controls as an evidence source. Choose the common controls that represent your goals, and use them as building blocks to create a control that collects evidence across your portfolio of compliance needs. Each automated common control maps to a predefined grouping of data sources. This means that you don't have to be an AWS expert to know which data sources collect the relevant evidence for your goals. And when you use common controls as an evidence source, you no longer have to maintain data source mappings, because Audit Manager handles this for you.

Create a vendor risk assessment question

You can use custom controls to support how you manage vendor risk assessments. Each control that you create can represent an individual risk assessment question. For example, the control name can be a question, and you can provide an answer by uploading a file or entering a text response as manual evidence.

Key points

When it comes to creating custom controls in Audit Manager, you have two methods to choose from:

1. **Creating a control from scratch** - This method provides maximum flexibility and enables you to tailor the control to your exact needs. This is a good option when you have a specific compliance

requirement that isn't adequately covered by an existing control. This method is particularly useful when you need to map your organization's enterprise controls to predefined groupings of AWS data sources or when you want to create vendor risk assessment questions as individual controls.

2. **Making an editable copy of an existing control** - If an existing standard control or custom control partially meets your needs, you can make an editable copy of that control. This approach is more efficient if you only need to make minor changes to an existing control. This is a good option if you want to adjust a few attributes to better align the control with your specific requirements. For example, you might change how often a control uses an API call to collect evidence, and then change the control's name to reflect this.

Additional resources

For instructions on how to create a custom control, see the following resources.

- Creating a custom control from scratch in AWS Audit Manager
- Making an editable copy of a control in AWS Audit Manager

Creating a custom control from scratch in AWS Audit Manager

When your organization's compliance requirements don't align with the pre-built standard controls that are available in AWS Audit Manager, you can create your own custom control from scratch.

This page outlines the steps to create a custom control that's tailored to your specific needs.

Prerequisites

Make sure your IAM identity has appropriate permissions to create a custom control in AWS Audit Manager. Two suggested policies that grant these permissions are AWSAuditManagerAdministratorAccess and Allow users management access to AWS Audit Manager.

To successfully collect evidence from AWS Config and Security Hub, make sure that you do the following:

- Enable AWS Config, then apply the required settings for using AWS Config with Audit Manager

- Enable Security Hub, then apply the required settings for using Security Hub with Audit Manager

Audit Manager can then collect evidence each time an evaluation occurs for a given AWS Config rule or Security Hub control.

Procedure

Tasks

- Step 1: Specify control details
- Step 2: Specify evidence sources
- Step 3 (Optional): Define action plan
- Step 4: Review and create the control

Step 1: Specify control details

Start by specifying the details of your custom control.

> **Important**
>
> We strongly recommend that you never put sensitive identifying information into free-form fields such as **Control details** or **Testing information**. If you create custom controls that contain sensitive information, you can't share any of your custom frameworks that contain these controls.

To specify control details

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the navigation pane, choose **Control library**, and then choose **Create custom control**.
3. Under **Control details**, enter the following information about the control.
   - **Control** – Enter a friendly name, a title, or a risk assessment question. This value helps you to identify your control in the control library.
   - **Description (optional)** – Enter details to help others understand the control's objective. This description appears on the control details page.

4. Under **Testing information**, enter the recommended steps for testing the control.
5. Under **Tags**, choose **Add new tag** to associate a tag with the control. You can specify a key for each tag that best describes the compliance framework that this control supports. The tag key is mandatory and can be used as a search criteria when you search for this control in the control library.
6. Choose **Next**.

Step 2: Specify evidence sources

Next, specify some evidence sources. An evidence source determines where your custom control collects evidence from. You can use AWS managed sources, customer managed sources, or both.

> **Tip**
>
> We recommend that you use AWS managed sources. Whenever an AWS managed source is updated, the same updates are automatically applied to all custom controls that use these sources. This means that your custom controls collect evidence against the latest definitions of that evidence source.

If you're not sure which options to choose, see the following examples and our recommendations.

Your role	Your goal	Recommended evidence source
GRC professional	I want to collect evidence for a particular domain or objective	AWS managed (common control) Use a predefined grouping of data sources that map to a specific common control.
Technical expert	I want to collect evidence about the AWS resources I'm responsible for	AWS managed (core control) Use a predefined grouping of data sources that map to an AWS requirement.

Your role	Your goal	Recommended evidence source
Technical expert	I want to use a custom AWS Config rule to collect evidence	Customer managed (Automated data source) Use a custom data source to collect specific automated evidence.
GRC professional	I want to collect evidence, such as documents and text responses	Customer managed (Manual data source) Use a custom data source to upload your own manual evidence.

To specify an AWS managed source (recommended)

We recommend that you start by choosing one or more common controls. When you choose the common control that represents your goal, Audit Manager collects the relevant evidence for all of the supporting core controls. You can also choose individual core controls if you want to collect targeted evidence about your AWS environment.

To specify an AWS managed source

1. Go to the **AWS managed sources** section of the page.
2. To add a common control, follow these steps:
    a. Select **Use a common control that matches your compliance goal**.
    b. Choose a common control from the dropdown list.
    c. (Optional) Repeat step 2 as needed. You can add up to five common controls.
3. To remove a common control, choose the **X** next to the control name.
4. To add a core control, follow these steps:
    a. Select **Use a core control that matches a prescriptive AWS guideline**.
    b. Choose a common control from the dropdown list.

c. (Optional) Repeat step 4 as needed. You can add up to 50 core controls.

5. To remove a core control, choose the **X** next to the control name.
6. To add customer managed data sources, use the following procedure. Otherwise, choose **Next**.

To specify a customer managed source

To collect automated evidence from a data source, you must choose a data source type and a data source mapping. These details map to your AWS usage, and tell Audit Manager where to collect the evidence from. If you want to provide your own evidence, you'll choose a manual data source instead.

> **Note**
>
> You're responsible for maintaining the data source mappings that you create in this step.

To specify a customer managed source

1. Go to the **Customer managed sources** section of the page.
2. Select **Use a data source to collect manual or automated evidence**.
3. Choose **Add**.
4. Choose one of the following options:

   - Choose **AWS API calls**, then choose an API call and an evidence collection frequency.
   - Choose **AWS CloudTrail event**, then choose an event name.
   - Choose **AWS Config managed rule**, then choose a rule identifier.
   - Choose **AWS Config custom rule**, then choose a rule identifier.
   - Choose **AWS Security Hub control**, then choose a Security Hub control.
   - Choose **Manual data source**, then choose an option:
     - **File upload** – Use this option if the control requires documentation as evidence.
     - **Text response** – Use this option if the control requires an answer to a risk assessment question.

> **Tip**
>
> For information about automated data source types and troubleshooting tips, see Supported data source types for automated evidence.
> If you need to validate your data source setup with an expert, choose **Manual data source** for now. That way, you can create the control and add it to a framework now, and then edit the control as needed later.

5. Under **Data source name**, provide a descriptive name.
6. (Optional) Under **Additional details**, enter a data source description and a troubleshooting description.
7. Choose **Add data source**.
8. (Optional) To add another data source, choose **Add** and repeat steps 1-7. You can add up to 100 data sources.
9. To remove a data source, select the data source from the table, then choose **Remove**.
10. When you're finished, choose **Next**.

Step 3 (Optional): Define action plan

Next, specify the actions to take if this control needs to be remediated.

> **Important**
>
> We strongly recommend that you never put sensitive identifying information into free-form fields such as **Action plan**. If you create custom controls that contain sensitive information, you can't share any of your custom frameworks that contain these controls.

To define action plan

1. Under **Title**, enter a descriptive title for the action plan.
2. Under **Instructions**, enter detailed instructions for the action plan.
3. Choose **Next**.

Step 4: Review and create the control

Review the information for the control. To change the information for a step, choose **Edit**.

When you're finished, choose **Create custom control**.

Next steps

After you create a new custom control, you can add it to a custom framework. To learn more, see Creating a custom framework in AWS Audit Manager or Editing a custom framework in AWS Audit Manager.

After you add the custom control to a custom framework, you can create an assessment and start collecting evidence. To learn more, see Creating an assessment in AWS Audit Manager.

To revisit your custom control at a later date, see Finding the available controls in AWS Audit Manager. You can follow these steps to locate your custom control so that you can view, edit, or delete it.

Additional resources

For solutions to control issues in Audit Manager, see Troubleshooting control and control set issues.

Making an editable copy of a control in AWS Audit Manager

Instead of creating a custom control from scratch, you can use an existing standard control or custom control as a starting point and make an editable copy that meets your needs. When you do this, the existing standard control remains in the control library, and a new control is created with your custom settings.

Prerequisites

Make sure your IAM identity has appropriate permissions to create a custom framework in AWS Audit Manager. Two suggested policies that grant these permissions are AWSAuditManagerAdministratorAccess and Allow users management access to AWS Audit Manager.

To successfully collect evidence from AWS Config and Security Hub, make sure that you do the following:

- Enable AWS Config, then apply the required settings for using AWS Config with Audit Manager.
- Enable Security Hub, then apply the required settings for using Security Hub with Audit Manager.

Audit Manager can then collect evidence each time an evaluation occurs for a given AWS Config rule or Security Hub control.

Procedure

Tasks

- Step 1: Specify control details
- Step 2: Specify evidence sources
- Step 3: (Optional): Define an action plan
- Step 4: Review and create the control

Step 1: Specify control details

The control details are inherited from the original control. Review and modify these details as needed.

> **Important**
>
> We strongly recommend that you never put sensitive identifying information into free-form fields such as **Control details** or **Testing information**. If you create custom controls that contain sensitive information, you can't share any of your custom frameworks that contain these controls.

To specify control details

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the navigation pane, choose **Control library**.
3. Select the standard control or custom control that you want to make changes to, and then choose **Make a copy**.
4. Specify the new name of the control, and choose **Continue**.

5. Under **Control details**, customize the control details as needed.
6. Under **Testing information**, make changes to the instructions as needed.
7. Under **Tags**, customize the tags as needed.
8. Choose **Next**.

Step 2: Specify evidence sources

Evidence sources are inherited from the original control. You can change, add, or remove evidence sources as needed.

To specify an AWS managed source (recommended)

> **Tip**
>
> We recommend that you start by choosing one or more common controls. If you have more fine-grained compliance requirements, you can also choose one or more specific core controls.

To specify an AWS managed source

1. Under **AWS managed sources**, review the current selections and make changes as needed.
2. To add a common control, follow these steps:
   a. Select **Use a common control that matches your compliance goal**.
   b. Choose a common control from the dropdown list.
   c. (Optional) Repeat step 2 as needed. You can add up to five common controls.
3. To remove a common control, choose the **X** next to the control name.
4. To add a core control, follow these steps:
   a. Select **Use a core control that matches a prescriptive AWS guideline**.
   b. Choose a common control from the dropdown list.
   c. (Optional) Repeat step 4 as needed. You can add up to 50 core controls.
5. To remove a core control, choose the **X** next to the control name.
6. To edit customer managed data sources, use the following procedure. Otherwise, choose **Next**.

To specify a customer managed source

To collect automated evidence from a data source, you must choose a data source type and a data source mapping. These details map to your AWS usage, and tell Audit Manager where to collect the evidence from. If you want to provide your own evidence, you'll choose a manual data source instead.

> **Note**
>
> You're responsible for maintaining the data source mappings that you create in this step.

To specify a customer managed source

1. Under **Customer managed sources**, review the current data sources and make changes as needed.
2. To remove a data source, select a data source from the table and choose **Remove**.
3. To add a new data source, follow these steps:
   a. Select **Use a data source to collect manual or automated evidence**.
   b. Choose **Add**.
   c. Choose one of the following options:
      - Choose **AWS API calls**, then choose an API call and an evidence collection frequency.
      - Choose **AWS CloudTrail event**, then choose an event name.
      - Choose **AWS Config managed rule**, then choose a rule identifier.
      - Choose **AWS Config custom rule**, then choose a rule identifier.
      - Choose **AWS Security Hub control**, then choose a Security Hub control.
      - Choose **Manual data source**, then choose an option:
        - **File upload** – Use this option if the control requires documentation as evidence.
        - **Text response** – Use this option if the control requires an answer to a risk assessment question.

> **Tip**
>
> For information about automated data source types and troubleshooting tips, see Supported data source types for automated evidence.
> If you need to validate your data source setup with an expert, choose **Manual data source** for now. That way, you can create the control and add it to a framework now, and then edit the control as needed later.

d. Under **Data source name**, provide a descriptive name.

e. (Optional) Under **Additional details**, enter a data source description and a troubleshooting description.

f. Choose **Add data source**.

g. (Optional) To add another data source, choose **Add** and repeat step 3. You can add up to 100 data sources.

4. When you're finished, choose **Next**.

Step 3: (Optional): Define an action plan

The action plan is inherited from the original control. You can edit this action plan as needed.

> **Important**
>
> We strongly recommend that you never put sensitive identifying information into free-form fields such as **Action plan**. If you create custom controls that contain sensitive information, you can't share any of your custom frameworks that contain these controls.

To specify instructions

1. Under **Title**, review the title and make changes as needed.
2. Under **Instructions**, review the instructions and make changes as needed.
3. Choose **Next**.

Step 4: Review and create the control

Review the information for the control. To change the information for a step, choose **Edit**. When you're finished, choose **Create custom control**.

Next steps

After you create a new custom control, you can add it to a custom framework. To learn more, see Creating a custom framework in AWS Audit Manager or Editing a custom framework in AWS Audit Manager.

After you add a custom control to a custom framework, you can create an assessment and start collecting evidence. To learn more, see Creating an assessment in AWS Audit Manager.

To revisit your custom control at a later date, see Finding the available controls in AWS Audit Manager. You can follow these steps to locate your custom control so that you can view, edit, or delete it.

Additional resources

For solutions to control issues in Audit Manager, see Troubleshooting control and control set issues.

Editing a custom control in AWS Audit Manager

You might need to modify your custom controls in AWS Audit Manager as your compliance requirements change.

This page outlines the steps to edit a custom control's details, evidence sources, and action plan instructions.

Prerequisites

The following procedure assumes that you have previously created a custom control.

Make sure your IAM identity has appropriate permissions to edit a custom control in AWS Audit Manager. Two suggested policies that grant these permissions are AWSAuditManagerAdministratorAccess and Allow users management access to AWS Audit Manager.

Procedure

Follow these steps to edit a custom control.

> **Note**
>
> When you edit a control, your changes are applied to all assessments where the control is active. In all of those assessments, Audit Manager will automatically start to collect evidence according to the latest control definition.

Tasks

- Step 1: Edit control details
- Step 2: Edit evidence sources
- Step 3: Edit action plan

Step 1: Edit control details

Review and edit the control details as needed.

> **Important**
>
> We strongly recommend that you never put sensitive identifying information into free-form fields such as **Control details** or **Testing information**. If you create custom controls that contain sensitive information, you can't share any of your custom frameworks that contain these controls.

To edit control details

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the navigation pane, choose **Control library** and then choose the **Custom** tab.
3. Select the control that you want to edit and then choose **Edit**.
4. Under **Control details**, edit the control details as needed.

5. Under **Testing information**, edit the description as needed.
6. Choose **Next**.

Step 2: Edit evidence sources

Next, you can edit, remove, or add evidence sources for the control.

> **Note**
>
> When you edit a control to include more or fewer evidence sources, this might affect how much evidence your control collects in any assessments where it's active. For example, if you add evidence sources, you might notice that Audit Manager performs more resource assessments and collects more evidence than before. If you remove evidence sources, it's likely that your control will collect less evidence moving forward.
> For more information about resource assessments and pricing, see AWS Audit Manager Pricing.

To edit an AWS managed source

To edit an AWS managed source

1. Under **AWS managed sources**, review the current selections and make changes as needed.
2. To add a common control, follow these steps:
   a. Select **Use a common control that matches your compliance goal**.
   b. Choose a common control from the dropdown list.
   c. (Optional) Repeat step 2 as needed. You can add up to five common controls.
3. To remove a common control, choose the **X** next to the control name.
4. To add a core control, follow these steps:
   a. Select **Use a core control that matches a prescriptive AWS guideline**.
   b. Choose a common control from the dropdown list.
   c. (Optional) Repeat step 4 as needed. You can add up to 50 core controls.
5. To remove a core control, choose the **X** next to the control name.
6. To add customer managed data sources, use the following procedure. Otherwise, choose **Next**.

To edit a customer managed source

> **Note**
>
> You're responsible for maintaining the data source mappings that you edit in this step.

To edit a customer managed source

1. Under **Customer managed sources**, review the current data sources and make changes as needed.
2. To remove a data source, select a data source from the table, then choose **Remove**.
3. To add a new data source, follow these steps:

   a. Select **Use a data source to collect manual or automated evidence**.

   b. Choose **Add**.

   c. Choose one of the following options:

   - Choose **AWS API calls**, then choose an API call and an evidence collection frequency.
   - Choose **AWS CloudTrail event**, then choose an event name.
   - Choose **AWS Config managed rule**, then choose a rule identifier.
   - Choose **AWS Config custom rule**, then choose a rule identifier.
   - Choose **AWS Security Hub control**, then choose a Security Hub control.
   - Choose **Manual data source**, then choose an option:
     - **File upload** – Use this option if the control requires documentation as evidence.
     - **Text response** – Use this option if the control requires an answer to a risk assessment question.

> **Tip**
>
> For information about automated data source types and troubleshooting tips, see Supported data source types for automated evidence.
> If you need to validate your data source setup with an expert, choose **Manual data source** for now. That way, you can create the control and add it to a framework now, and then edit the control as needed later.

d. Under **Data source name**, provide a descriptive name.

e. (Optional) Under **Additional details**, enter a data source description and a troubleshooting description.

f. Choose **Add data source**.

g. (Optional) To add another data source, choose **Add** and repeat step 3. You can add up to 100 data sources.

4. When you're finished, choose **Next**.

Step 3: Edit action plan

Next, review and edit the optional action plan.

> **Important**
>
> We strongly recommend that you never put sensitive identifying information into free-form fields such as **Action plan**. If you create custom controls that contain sensitive information, you can't share any of your custom frameworks that contain these controls.

To edit an action plan

1. Under **Title**, edit the title as needed.
2. Under **Instructions**, edit the instructions as needed.
3. Choose **Next**.

Step 4: Review and save

Review the information for the control. To change the information for a step, choose **Edit**.

When you're finished, choose **Save changes**.

> **Note**
>
> After you edit a control, the changes take effect as follows in all active assessments that include the control:

- For controls with *AWS API calls* as the data source type, changes take effect at 00:00 UTC the following day.
- For all other controls, changes take effect immediately.

Next steps

When you're certain that you no longer need a custom control, you can clean up your Audit Manager environment by deleting the control. For instructions, see Deleting a custom control in AWS Audit Manager.

Additional resources

For solutions to control issues in Audit Manager, see Troubleshooting control and control set issues.

Changing how often a control collects evidence

AWS Audit Manager can collect evidence from various data sources. The frequency of evidence collection depends on the type of data source that the control uses.

The following sections provide more information about the evidence collection frequency for each control data source type, and how to change it (if applicable).

Topics

Key points

- For **AWS API calls**, Audit Manager collects evidence using a describe API call to another AWS service. You can specify the evidence collection frequency directly in Audit Manager (for custom controls only).

- For **AWS Config**, Audit Manager reports the result of a compliance check directly from AWS Config. The frequency follows the triggers that are defined in the AWS Config rule.
- For **AWS Security Hub**, Audit Manager reports the result of a compliance check directly from Security Hub. The frequency follows the schedule of the Security Hub check.
- For **AWS CloudTrail**, Audit Manager collects evidence continuously from CloudTrail. You can't change the frequency for this evidence type.

Configuration snapshots from AWS API calls

> **Note**
>
> The following applies only to custom controls. You can't change the evidence collection frequency for a standard control.

If a custom control uses AWS API calls as a data source type, you can change the evidence collection frequency in Audit Manager by following these steps.

To change the evidence collection frequency for a custom control with an API call data source

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the navigation pane, choose **Control library**, and then choose the **Custom** tab.
3. Choose the custom control that you want to edit, and then choose **Edit**.
4. On the **Edit control details** page, choose **Next**.
5. Under **Customer managed sources**, look for the API call data source that you want to update.
6. Select the data source from the table, then choose **Remove**.
7. Choose **Add**.
8. Choose **AWS API calls**.
9. Choose the same API call that you removed in step 5, and then select your preferred evidence collection frequency.
10. Under **Data source name**, provide a descriptive name.
11. (Optional) Under **Additional details**, enter a data source description and a troubleshooting description.

12. Choose **Next**.
13. On the **Edit an action plan** page, choose **Next**.
14. On the **Review and update** page, review the information for the custom control. To change the information for a step, choose **Edit**.
15. When you're finished, choose **Save changes**.

After you edit a control, the changes take effect at 00:00 UTC the following day in all active assessments that include the control.

Compliance checks from AWS Config

> **Note**
>
> The following applies to both standard controls and custom controls that use AWS Config Rules as a data source.

If a control uses AWS Config as a data source type, you can't change the evidence collection frequency directly in Audit Manager. This is because the frequency follows the triggers that are defined in the AWS Config rule.

There are two types of triggers for AWS Config Rules:

1. **Configuration changes** - AWS Config runs evaluations for the rule when certain types of resources are created, changed, or deleted.
2. **Periodic** - AWS Config runs evaluations for the rule at a frequency that you choose (for example, every 24 hours).

To learn more about the triggers for AWS Config Rules, see Trigger types in the *AWS Config Developer Guide*.

For instructions on how to manage AWS Config Rules, see Managing your AWS Config rules.

Compliance checks from Security Hub

> **Note**
>
> The following applies to both standard controls and custom controls that use Security Hub checks as a data source.

If a control uses Security Hub as a data source type, you can't change the evidence collection frequency directly in Audit Manager. This is because the frequency follows the schedule of the Security Hub checks.

- **Periodic checks** run automatically within 12 hours after the most recent run. You cannot change the periodicity.
- **Change-triggered checks** run when the associated resource changes state. Even if the resource doesn't change state, the updated at time for change-triggered checks is refreshed every 18 hours. This helps to indicate that the control is still enabled. In general, Security Hub uses change-triggered rules whenever possible.

To learn more, see Schedule for running security checks in the *AWS Security Hub User Guide*.

User activity logs from AWS CloudTrail

> **Note**
>
> The following applies to both standard controls and custom controls that use AWS CloudTrail user activity logs as a data source.

You can't change the evidence collection frequency for controls that use activity logs from CloudTrail as a data source type. Audit Manager collects this evidence type from CloudTrail in a continuous manner. The frequency is continuous because user activity can happen at any time of the day.

Deleting a custom control in AWS Audit Manager

If you created a custom control and you no longer need it, you can delete it from your Audit Manager environment. This enables you to clean up your workspace and focus on the custom controls that are relevant to your current tasks and priorities.

Prerequisites

The following procedure assumes that you have previously created a custom control.

Make sure your IAM identity has appropriate permissions to delete a custom control in AWS Audit Manager. Two suggested policies that grant these permissions are AWSAuditManagerAdministratorAccess and Allow users management access to AWS Audit Manager.

Procedure

You can delete custom controls using the Audit Manager console, the Audit Manager API, or the AWS Command Line Interface (AWS CLI).

> **Important**
>
> When you delete a custom control, this action removes the control from any custom frameworks or assessments that it's currently related to. As a result, Audit Manager will stop collecting evidence for that custom control in all of your assessments. This includes assessments that you previously created before you deleted the custom control.

Audit Manager console

To delete a custom control on the Audit Manager console

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the navigation pane, choose **Control library** and then choose the **Custom controls** tab.
3. Select the control that you want to delete, and then choose **Delete**.
4. In the pop-up window that appears, choose **Delete** to confirm deletion.

AWS CLI

To delete a custom control in the AWS CLI

1. First, identify the custom control that you want to delete. To do this, run the list-controls command and specify the `--control-type` as `Custom`.

   ```
   aws auditmanager list-controls --control-type Custom
   ```

   The response returns a list of custom controls. Find the control that you want to delete, and take note of the control ID.
2. Next, run the delete-control command and use the `--control-id` parameter to specify the control that you want to delete.

   In the following example, replace the *`placeholder text`* with your own information.

   ```
   aws auditmanager delete-control --control-id a1b2c3d4-5678-90ab-cdef-
   EXAMPLE11111
   ```

Audit Manager API

To delete a custom control using the API

1. Use the ListControls operation and specify the controlType as `Custom`. From the response, find the control that you want to delete and note the control ID.
2. Use the DeleteControl operation to delete the custom control. In the request, use the controlId parameter to specify the control that you want to delete.

For more information about these API operations, choose any of the links in the previous procedure to read more in the *AWS Audit Manager API Reference*. This includes information about how to use these operations and parameters in one of the language-specific AWS SDKs.

Additional resources

For information about data retention in Audit Manager, see Deletion of Audit Manager data.

Reviewing and configuring your AWS Audit Manager settings

You can review and configure your AWS Audit Manager settings at any time to ensure that they meet your specific needs.

This chapter takes you through the process of accessing, reviewing, and adjusting your Audit Manager settings step-by-step. By following along, you'll learn how to change your general settings, assessment settings, and evidence finder settings to align with your evolving compliance goals and business requirements.

Procedure

To get started, follow these steps to view your Audit Manager settings. You can view your Audit Manager settings using the Audit Manager console, the AWS Command Line Interface (AWS CLI), or the Audit Manager API.

To view your settings

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the left navigation pane, choose **Settings**.
3. Choose the tab that meets your goal.

   - **General settings** - Choose this tab to review and update your general Audit Manager settings.
   - **Assessment settings** - Choose this tab to review and update the default settings for your assessments.
   - **Evidence finder settings** - Choose this tab to review and update your evidence finder settings.

Next steps

To customize your Audit Manager settings for your use case, follow the procedures that are outlined here.

- **General settings**
  - Configuring your data encryption settings
  - Adding a delegated administrator
  - Changing a delegated administrator
  - Removing a delegated administrator
  - Disabling AWS Audit Manager
- **Assessment settings**
  - Configuring your default audit owners
  - Configuring your default assessment report destination
  - Configuring your Audit Manager notifications
- **Evidence finder settings**
  - Enabling evidence finder
  - Confirming the status of evidence finder
  - Configuring your default export destination for evidence finder
  - Disabling evidence finder

Configuring your data encryption settings

You can choose how you encrypt your data in AWS Audit Manager. Audit Manager automatically creates a unique AWS managed key for the secure storage of your data. By default, your Audit Manager data is encrypted with this KMS key. However, if you want to customize your data encryption settings, you can specify your own symmetric encryption customer managed key. Using your own KMS key gives you more flexibility, including the ability to create, rotate, and disable keys.

Prerequisites

If you provide a customer managed key, it must be in the same AWS Region as your assessment in order to generate assessment reports and export evidence finder search results successfully.

Procedure

You can update your data encryption settings using the Audit Manager console, the AWS Command Line Interface (AWS CLI), or the Audit Manager API.

> **Note**
>
> When you change your Audit Manager data encryption settings, these changes apply to any new assessments that you create. This includes any assessment reports and evidence finder exports that you create from your new assessments.
>
> The changes don't apply to existing assessments that you created before you changed your encryption settings. This includes new assessment reports and CSV exports that you create from existing assessments, in addition to existing assessment reports and CSV exports. Existing assessments—and all their assessment reports and CSV exports—continue to use the old KMS key. If the IAM identity that generates the assessment report can't use the old KMS key, grant permissions at the key policy level.

Audit Manager console

To update your data encryption settings on the Audit Manager console

1. From the **General** settings tab, go to the **Data encryption** section.
2. To use the default KMS key that's provided by Audit Manager, clear the **Customize encryption settings (advanced)** check box.
3. To use a customer managed key, select the **Customize encryption settings (advanced)** check box. You can then choose an existing KMS key, or create a new one.

AWS CLI

To update your data encryption settings in the AWS CLI

Run the update-settings command and use the `--kms-key` parameter to specify your own customer managed key.

In the following example, replace the *`placeholder text`* with your own information.

```
aws auditmanager update-settings --kms-key arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

Audit Manager API

To update your data encryption settings using the API

Call the UpdateSettings operation and use the kmsKey parameter to specify your own customer managed key.

For more information, choose the previous links to read more in the *Audit Manager API Reference*. This includes information about how to use this operation and parameter in one of the language-specific AWS SDKs.

Additional resources

- For instructions on how to create keys, see Creating keys in the *AWS Key Management Service User Guide*.
- For instructions on how to grant permissions at the key policy level, see Allowing users in other accounts to use a KMS key in the *AWS Key Management Service Developer Guide*.

Adding a delegated administrator

If you use AWS Organizations and want to enable multi-account support for AWS Audit Manager, you can designate a member account in your organization as the delegated administrator for Audit Manager.

If you want to use Audit Manager in more than one AWS Region, you must designate a delegated administrator account separately in each Region. In your Audit Manager settings, you should use the same delegated administrator account across all Regions.

Prerequisites

Take note of the following factors that define how the delegated administrator operates in Audit Manager:

- Your account must be part of an organization.
- Before you designate a delegated administrator, you must enable all features in your organization. You must also configure your organization's Security Hub settings. This way, Audit Manager can collect Security Hub evidence from your member accounts.
- The delegated administrator account must have access on the KMS key that you provided when setting up Audit Manager.

- You can't use your AWS Organizations management account as a delegated administrator in Audit Manager.

Procedure

You can add a delegated administrator using the Audit Manager console, the AWS Command Line Interface (AWS CLI), or the Audit Manager API.

> **Note**
>
> After you add a delegated administrator in your Audit Manager settings, your management account can no longer create additional assessments in Audit Manager. Additionally, evidence collection stops for any existing assessments created by the management account. Audit Manager collects and attaches evidence to the delegated administrator account, which is the main account for managing your organization's assessments.

Audit Manager console

To add a delegated administrator on the Audit Manager console

1. From the **General** settings tab, go to the **Delegated administrator** section.
2. Under **Delegated administrator account ID**, enter the account ID of the delegated administrator.
3. Choose **Delegate**.

AWS CLI

To add a delegated administrator in the AWS CLI

Run the register-organization-admin-account command and use the `--admin-account-id` parameter to specify the account ID of the delegated administrator.

In the following example, replace the *`placeholder text`* with your own information.

```
aws auditmanager register-organization-admin-account --admin-account-id 111122223333
```

Audit Manager API

To add a delegated administrator using the API

Call the RegisterOrganizationAdminAccount operation and use the adminAccountId parameter to specify the account ID of the delegated administrator.

For more information, choose the previous links to read more in the *Audit Manager API Reference*. This includes information about how to use this operation and parameter in one of the language-specific AWS SDKs.

Next steps

To change your delegated administrator account, see Changing a delegated administrator.

To remove your delegated administrator account, see Removing a delegated administrator.

Additional resources

- Creating and managing an organization
- Troubleshooting delegated administrator and AWS Organizations issues

Changing a delegated administrator

Changing your delegated administrator in AWS Audit Manager is a two-step process. First, you need to remove the current delegated administrator account. Then, you can add a new account as the delegated administrator.

Follow the steps on this page to change your delegated administrator.

Contents

Prerequisites

Before you remove the current account

Before you remove the current delegated administrator account, keep in mind the following considerations:

- **Evidence finder cleanup task** - If the current delegated administrator (account A) enabled evidence finder, you'll need to perform a cleanup task before you assign account B as the new delegated administrator.

  Before you use your management account to remove account A, make sure that account A signs in to Audit Manager and disables evidence finder. Disabling evidence finder automatically deletes the event data store that was created in the account when evidence finder was enabled.

  If this task isn't completed, the event data store remains in account A. In this case, we recommend that the original delegated administrator uses CloudTrail Lake to manually delete the event data store.

  This cleanup task is necessary to ensure that you don't end up with multiple event data stores. Audit Manager ignores an unused event data store after you remove or change a delegated administrator account. However, if you don't delete the unused event data store, the event data store continues to incur storage costs from CloudTrail Lake.
- **Data deletion** - When you remove a delegated administrator account for Audit Manager, the data for that account isn't deleted. If you want to delete resource data for a delegated administrator account, you must perform that task separately before you remove the account. Either, you can do this in the Audit Manager console. Or, you can use one of the delete API operations that are provided by Audit Manager. For a list of available delete operations, see Deletion of Audit Manager data.

  At this time, Audit Manager doesn't provide an option to delete evidence for a specific delegated administrator. Instead, when your management account deregisters Audit Manager, we perform a cleanup for the current delegated administrator account at the time of deregistration.

Before you add the new account

Before you add the new delegated administrator account, keep in mind the following considerations:

- The new account must be part of an organization.
- Before you designate a new delegated administrator, you must enable all features in your organization. You must also configure your organization's Security Hub settings. This way, Audit Manager can collect Security Hub evidence from your member accounts.
- The delegated administrator account must have access on the KMS key that you provided when setting up Audit Manager.
- You can't use your AWS Organizations management account as a delegated administrator in Audit Manager.

Procedure

You can change a delegated administrator using the Audit Manager console, the AWS Command Line Interface (AWS CLI), or the Audit Manager API.

> **Warning**
>
> When you change a delegated administrator, you continue to have access to the evidence that you previously collected under the old delegated administrator account. However, Audit Manager stops collecting and attaching evidence to the old delegated administrator account.

Audit Manager console

To change the current delegated administrator on the Audit Manager console

1. (Optional) If the current delegated administrator (account A) enabled evidence finder, perform the following cleanup task:

   - Before assigning account B as the new delegated administrator, make sure that account A signs in to Audit Manager and disables evidence finder.

     Disabling evidence finder automatically deletes the event data store that was created when account A enabled evidence finder. If you don't complete this step, then account A must go to CloudTrail Lake and manually delete the event data store. Otherwise, the event data store remains in account A and continues to incur CloudTrail Lake storage charges.

2. From the **General** settings tab, go to the **Delegated administrator** section and choose **Remove**.
3. In the pop-up window that appears, choose **Remove** to confirm.
4. Under **Delegated administrator account ID**, enter the ID of the new delegated administrator account.
5. Choose **Delegate**.

AWS CLI

To change the current delegated administrator in the AWS CLI

First, run the deregister-organization-admin-account command using the `--admin-account-id` parameter to specify the account ID of the current delegated administrator.

In the following example, replace the *placeholder text* with your own information.

```
aws auditmanager deregister-organization-admin-account --admin-account-
id 111122223333
```

Then, run the register-organization-admin-account command using the `--admin-account-id` parameter to specify the account ID of the new delegated administrator.

In the following example, replace the *placeholder text* with your own information.

```
aws auditmanager register-organization-admin-account --admin-account-id 444455556666
```

Audit Manager API

To change the current delegated administrator using the API

First, call the DeregisterOrganizationAdminAccount operation and use the adminAccountId parameter to specify the account ID of the current delegated administrator.

Then, call the RegisterOrganizationAdminAccount operation and use the adminAccountId parameter to specify the account ID of the new delegated administrator.

For more information, choose the previous links to read more in the *Audit Manager API Reference*. This includes information about how to use this operation and parameter in one of the language-specific AWS SDKs.

Next steps

To remove your delegated administrator account, see Removing a delegated administrator.

Additional resources

- Creating and managing an organization
- Troubleshooting delegated administrator and AWS Organizations issues

Removing a delegated administrator

Removing the delegated administrator account stops further evidence collection for that account, but you retain access to the previously collected evidence.

If you need to remove your delegated administrator account for Audit Manager, you can follow the necessary steps on this page. Follow the prerequisites and procedures carefully, as they involve cleaning up resources to avoid unnecessary storage costs.

Prerequisites

Before you remove the delegated administrator account from Audit Manager, keep in mind the following considerations:

Evidence finder cleanup task

If the current delegated administrator enabled evidence finder, you need to perform a cleanup task.

Before you use your management account to remove the current delegated administrator, make sure that the current delegated administrator account signs in to Audit Manager and disables evidence finder. Disabling evidence finder automatically deletes the event data store that was created in the account when evidence finder was enabled.

If this task isn't completed, the event data store remains in their account. In this case, we recommend that the original delegated administrator uses CloudTrail Lake to manually delete the event data store.

This cleanup task is necessary to ensure that you don't end up with multiple event data stores. Audit Manager ignores an unused event data store after you remove or change a delegated

administrator account. However, if you don't delete the unused event data store, the event data store continues to incur storage costs from CloudTrail Lake.

Data deletion

When you remove a delegated administrator account for Audit Manager, the data for that account isn't deleted. If you want to delete resource data for a delegated administrator account, you must perform that task separately before you remove the account. Either, you can do this in the Audit Manager console. Or, you can use one of the delete API operations that are provided by Audit Manager. For a list of available delete operations, see Deletion of Audit Manager data.

At this time, Audit Manager doesn't provide an option to delete evidence for a specific delegated administrator. Instead, when your management account deregisters Audit Manager, we perform a cleanup for the current delegated administrator account at the time of deregistration.

Procedure

You can remove a delegated administrator using the Audit Manager console, the AWS Command Line Interface (AWS CLI), or the Audit Manager API.

> **Warning**
>
> When you remove a delegated administrator, you continue to have access to the evidence that you previously collected under that delegated administrator account. However, Audit Manager stops collecting and attaching evidence to the old delegated administrator account.

Audit Manager console

To remove the current delegated administrator on the Audit Manager console

1. (Optional) If the current delegated administrator enabled evidence finder, perform the following cleanup task:

   - Make sure that the current delegated administrator account signs in to Audit Manager and disables evidence finder.

Disabling evidence finder automatically deletes the event data store that was created in their account when they enabled evidence finder. If this step isn't completed, the delegated administrator account must use CloudTrail Lake to manually delete the event data store. Otherwise, the event data store remains in their account and continues to incur CloudTrail Lake storage charges.

2. From the **General** settings tab, go to the **Delegated administrator** section and choose **Remove**.
3. In the pop-up window that appears, choose **Remove** to confirm.

AWS CLI

Disabling evidence finder automatically deletes the event data store that was created in their account when they enabled evidence finder. If this step isn't completed, the delegated administrator account must use CloudTrail Lake to manually delete the event data store. Otherwise, the event data store remains in their account and continues to incur CloudTrail Lake storage charges.

To remove the current delegated administrator in the AWS CLI

Run the deregister-organization-admin-account command and use the `--admin-account-id` parameter to specify the account ID of the delegated administrator.

In the following example, replace the *`placeholder text`* with your own information.

```
aws auditmanager deregister-organization-admin-account --admin-account-
id 111122223333
```

Audit Manager API

To remove the current delegated administrator using the API

Call the DeregisterOrganizationAdminAccount operation and use the adminAccountId parameter to specify the account ID of the delegated administrator.

For more information, choose the previous links to read more in the *Audit Manager API Reference*. This includes information about how to use this operation and parameter in one of the language-specific AWS SDKs.

Additional resources

- Troubleshooting delegated administrator and AWS Organizations issues

Configuring your default audit owners

You can use this setting to specify the default audit owners who have primary access to your assessments in Audit Manager.

Procedure

You can update this setting using the Audit Manager console, the AWS Command Line Interface (AWS CLI), or the Audit Manager API.

Audit Manager console

You can choose from the AWS accounts listed in the table, or use the search bar to look for other AWS accounts.

To update your default audit owners on the Audit Manager console

1. From the **Assessment** settings tab, go to the **Default audit owners** section and choose **Edit**.
2. To add a default audit owner, select the check box next to the account name under **Audit owner**.
3. To remove a default audit owner, clear the check box next to the account name under **Audit owner**.
4. When you're done, choose **Save**.

AWS CLI

To update your default audit owner in the AWS CLI

Run the update-settings command and use the `--default-process-owners` parameter to specify an audit owner.

In the following example, replace the *`placeholder text`* with your own information. Note that `roleType` can only be `PROCESS_OWNER`.

```
aws auditmanager update-settings --default-process-owners
 roleType=PROCESS_OWNER,roleArn=arn:aws:iam::111122223333:role/Administrator
```

Audit Manager API

To update your default audit owner using the API

Call the UpdateSettings operation and use the defaultProcessOwners parameter to specify default audit owners. Note that `roleType` can only be `PROCESS_OWNER`.

Additional resources

- For more information about audit owners, see Audit owners in the *Concepts and terminology* section of this guide.

Configuring your default assessment report destination

When you generate an assessment report, Audit Manager publishes the report to the S3 bucket of your choice. This S3 bucket is referred to as an assessment report destination. You can choose the S3 bucket that Audit Manager stores your assessment reports in.

Prerequisites

Configuration tips for your assessment report destination

To ensure the successful generation of your assessment report, we recommend that you use the following configurations for your assessment report destination.

Same-Region buckets

We recommend that you use an S3 bucket that's in the same AWS Region as your assessment. When you use a same-Region bucket and assessment, your assessment report can include up to 22,000 evidence items. Conversely, when you use a cross-Region bucket and assessment, only 3,500 evidence items can be included.

AWS Region

The AWS Region of your customer managed key (if you provided one) must match the Region of your assessment and your assessment report destination S3 bucket. For instructions on how

to change the KMS key, see Configuring your data encryption settings. For a list of supported Audit Manager Regions, see AWS Audit Manager endpoints and quotas in the *Amazon Web Services General Reference*.

S3 bucket encryption

If your assessment report destination has a bucket policy that requires server-side encryption (SSE) using SSE-KMS, then the KMS key used in that bucket policy must match the KMS key that you configured in your Audit Manager data encryption settings. If you haven't configured a KMS key in your Audit Manager settings, and your assessment report destination bucket policy requires SSE, ensure that the bucket policy allows SSE-S3. For instructions on how to configure the KMS key that's used for data encryption, see Configuring your data encryption settings.

Cross-account S3 buckets

Using a cross-account S3 bucket as your assessment report destination isn't supported in the Audit Manager console. It's possible to specify a cross-account bucket as your assessment report destination by using the AWS CLI or one of the AWS SDKs, but for simplicity, we recommend that you not do this.

> **Tip**
>
> For optimal security and performance, we recommend using an S3 bucket in the same AWS account and region as your assessment.

If you do choose to use a cross-account S3 bucket as your assessment report destination, consider the following points.

- By default, S3 objects—such as assessment reports—are owned by the AWS account that uploads the object. You can use the S3 Object Ownership setting to change this default behavior so that any new objects that are written by accounts with the `bucket-owner-full-control` canned access control list (ACL) automatically become owned by the bucket owner.

  Although it's not a requirement, we recommend that you make the following changes to your cross-account bucket settings. Making these changes ensures that the bucket owner has full control of the assessment reports that you publish to their bucket.

  - Set the object ownership of the S3 bucket to *bucket owner preferred*, instead of the default *object writer*

- Add a bucket policy to ensure that objects uploaded to that bucket have the `bucket-owner-full-control` ACL

- To allow Audit Manager to publish reports in a cross-account S3 bucket, you must add the following S3 bucket policy to your assessment report destination. Replace the *`placeholder text`* with your own information. The `Principal` element in this policy is the user or role that owns the assessment and creates the assessment report. The `Resource` specifies the cross-account S3 bucket where the report is published.

  JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow cross account assessment report publishing",
            "Effect": "Allow",
            "Principal": {
                "AWS":
 "arn:aws:iam::111122223333:user/AssessmentOwnerUserName"
            },
            "Action": [
                "s3:ListBucket",
                "s3:PutObject",
                "s3:GetObject",
                "s3:GetBucketLocation",
                "s3:PutObjectAcl",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::CROSS-ACCOUNT-BUCKET",
                "arn:aws:s3:::CROSS-ACCOUNT-BUCKET/*"
            ]
        }
    ]
}
```

Procedure

You can update this setting using the Audit Manager console, the AWS Command Line Interface (AWS CLI), or the Audit Manager API.

Audit Manager console

To update your default assessment report destination on the Audit Manager console

1. From the **Assessment** settings tab, go to the **Assessment report destination** section.
2. To use an existing S3 bucket, select a bucket name from the dropdown menu.
3. To create a new S3 bucket, choose **Create new bucket**.
4. When you're done, choose **Save**.

AWS CLI

To update your default assessment report destination in the AWS CLI

Run the update-settings command and use the `--default-assessment-reports-destination` parameter to specify an S3 bucket.

In the following example, replace the *`placeholder text`* with your own information:

```
aws auditmanager update-settings --default-assessment-reports-destination
 destinationType=S3,destination=s3://amzn-s3-demo-destination-bucket
```

Audit Manager API

To update your default assessment report destination using the API

Call the UpdateSettings operation and use the defaultAssessmentReportsDestination parameter to specify an S3 bucket.

Additional resources

- Creating a bucket
- Assessment reports

Configuring your Audit Manager notifications

You can configure Audit Manager to send notifications to the Amazon SNS topic of your choice. If you're subscribed to that SNS topic, you receive notifications directly whenever you sign in to Audit Manager.

Follow the steps on this page to learn how to view and update your notification settings to suit your preferences. You can use either a standard SNS topic or a FIFO (first-in-first-out) SNS topic. Although Audit Manager supports sending notifications to FIFO topics, the order that messages are sent in isn't guaranteed.

Prerequisites

If you want to use an Amazon SNS topic that you don't own, you must configure your AWS Identity and Access Management (IAM) policy for this. More specifically, you must configure it to allow publishing from the Amazon Resource Name (ARN) of the topic. For an example policy that you can use, see Example 1 (Permissions for the SNS topic).

Procedure

You can update this setting using the Audit Manager console, the AWS Command Line Interface (AWS CLI), or the Audit Manager API.

Audit Manager console

To update your notification settings on the Audit Manager console

1. From the **Assessment** settings tab, go to the **Notifications** section.
2. To use an existing SNS topic, select the topic name from the dropdown menu.
3. To create a new SNS topic, choose **Create new topic**.
4. When you're done, choose **Save**.

AWS CLI

To update your notification settings in the AWS CLI

Run the update-settings command and use the `--sns-topic` parameter to specify an SNS topic.

In the following example, replace the *placeholder text* with your own information:

```
aws auditmanager update-settings --sns-topic arn:aws:sns:us-east-1:111122223333:my-assessment-topic
```

Audit Manager API

To update your notification settings using the API

Call the UpdateSettings operation and use the snsTopic parameter to specify an SNS topic.

Additional resources

- For instructions on how to create an Amazon SNS topic, see Creating an Amazon SNS topic in the *Amazon SNS User Guide*.
- For an example policy that you can use to allow Audit Manager to send notifications to Amazon SNS topics , see Example 1 (Permissions for the SNS topic)
- To learn more about the list of actions that invoke notifications in Audit Manager, see Notifications in AWS Audit Manager.
- For solutions to notification issues in Audit Manager, see Troubleshooting notification issues.

Enabling evidence finder

You can enable the evidence finder feature in Audit Manager to search for evidence in your AWS account. If you're a delegated administrator for Audit Manager, you can search for evidence for all member accounts in your organization.

Follow these steps to learn how to enable evidence finder. Pay close attention to the prerequisites, as you'll need specific permissions to create and manage an event data store in CloudTrail Lake for this functionality.

Prerequisites

Required permissions to enable evidence finder

To enable evidence finder, you need permissions to create and manage an event data store in CloudTrail Lake. To use the feature, you need permissions to perform CloudTrail Lake queries. For an example permission policy that you can use, see Example 3 (Permissions to enable evidence finder).

If you need help with permissions, contact your AWS administrator. If you're an AWS administrator, you can copy the required permission statement and attach it to an IAM policy.

Procedure

Requesting to enable evidence finder

You can complete this task using the Audit Manager console, the AWS Command Line Interface (AWS CLI), or the Audit Manager API.

> **Note**
>
> You must enable evidence finder in each AWS Region where you want to search for evidence.

Audit Manager console

To request to enable evidence finder on the Audit Manager console

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. From the **Evidence finder** settings tab, go to the **Evidence finder** section.
3. Choose **Required permission policy**, then **View CloudTrail Lake permissions** to view the required evidence finder permissions. If you don't already have these permissions, you can copy this policy statement and attach it to an IAM policy.
4. Choose **Enable**.
5. In the pop-up window, choose **Request to enable**.

AWS CLI

To request to enable evidence finder in the AWS CLI

Run the update-settings command with the `--evidence-finder-enabled` parameter.

```
aws auditmanager update-settings --evidence-finder-enabled
```

Audit Manager API

To request to enable evidence finder using the API

Call the UpdateSettings operation and use the evidenceFinderEnabled parameter.

For more information, choose the previous links to read more in the *Audit Manager API Reference*. This includes information about how to use this operation and parameter in one of the language-specific AWS SDKs.

Next steps

After you've requested to enable evidence finder, you can check the status of your request. For instructions, see Confirming the status of evidence finder.

Additional resources

- Evidence finder
- Troubleshooting evidence finder issues

Confirming the status of evidence finder

After you submit your request to enable evidence finder, it takes up to 10 minutes to enable the feature and create an event data store. As soon as the event data store is created, all new evidence is ingested into the event data store moving forward.

When evidence finder is enabled and the event data store is created, we backfill the newly created event data store with up to two years' worth of your past evidence. This process happens automatically and takes up to seven days to complete.

Follow the steps on this page to check and understand the status of your request to enable evidence finder.

Prerequisites

Make sure that you followed the steps to enable evidence finder. For instructions, see Enabling evidence finder.

Procedure

You can check the current status of evidence finder using the Audit Manager console, the AWS CLI, or the Audit Manager API.

Audit Manager console

To see the current status of evidence finder on the Audit Manager console

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the left navigation pane, choose **Settings**.
3. Under **Enable evidence finder – optional**, review the current status.

   Each status is defined as follows:

Status	Description
Evidence finder isn't enabled	You haven't successfully enabled evidence finder yet.
You have requested to enable evidence finder	Your request is pending the event data store being created.
Evidence finder is enabled	The event data store was created. You can now use evidence finder. Depending how much evidence you have, it takes up to seven days to backfill the new event data store with your past evidence data. A blue information panel indicates that the data backfill is in progress. Feel free to start exploring evidence finder in the meantime. However, keep in mind that not all data is available until the backfill is complete.
You have requested to disable evidence finder	Your request is pending the event data store being deleted.
Evidence finder has been disabled	Evidence finder has been permanently disabled and the event data store is deleted.

AWS CLI

To see the current status of evidence finder in the AWS CLI

Run the get-settings command with the `--attribute` parameter set to `EVIDENCE_FINDER_ENABLEMENT`.

```
aws auditmanager get-settings --attribute EVIDENCE_FINDER_ENABLEMENT
```

This returns the following information:

enablementStatus

This attribute shows the current status of evidence finder.

- `ENABLE_IN_PROGRESS` – You requested to enable evidence finder. An event data store is currently being created to support evidence finder queries.
- `ENABLED` – An event data store was created and evidence finder is enabled. We recommend waiting seven days until the event data store is backfilled with your past evidence data. You can use evidence finder in the meantime, but not all data is available until the backfill is complete.
- `DISABLE_IN_PROGRESS` – You requested to disable evidence finder, and your request is pending the event data store being deleted.
- `DISABLED` – You permanently disabled evidence finder and the event data store is deleted. You can't re-enable evidence finder after this point.

backfillStatus

This attribute shows the current status of the evidence data backfill.

- `NOT_STARTED` – The backfill hasn't started yet.
- `IN_PROGRESS` – The backfill is in progress. This takes up to seven days to complete, depending on the amount of evidence data.
- `COMPLETED` – The backfill is complete. All of your past evidence is now queryable.

Audit Manager API

To see the current status of evidence finder using the API

Call the GetSettings operation with the `attribute` parameter set to `EVIDENCE_FINDER_ENABLEMENT`. This returns the following information:

enablementStatus

This attribute shows the current status of evidence finder.

- `ENABLE_IN_PROGRESS` - You requested to enable evidence finder. An event data store is currently being created to support evidence finder queries.
- `ENABLED` - An event data store was created and evidence finder is enabled. We recommend waiting seven days until the event data store is backfilled with your past evidence data. You can use evidence finder in the meantime, but not all data is available until the backfill is complete.
- `DISABLE_IN_PROGRESS` - You requested to disable evidence finder, and your request is pending the deletion of the event data store.
- `DISABLED` - You permanently disabled evidence finder and the event data store is deleted. You can't re-enable evidence finder after this point.

backfillStatus

This attribute shows the current status of the evidence data backfill.

- `NOT_STARTED` means that the backfill hasn't started yet.
- `IN_PROGRESS` means that the backfill is in progress. This takes up to seven days to complete, depending on the amount of evidence data.
- `COMPLETED` means that the backfill is complete. All of your past evidence is now queryable.

For more information, see evidenceFinderEnablement in the *Audit Manager API Reference*.

Next steps

After evidence finder is successfully enabled, you can start using the feature. We recommend waiting seven days until the event data store is backfilled with your past evidence data. You can use evidence finder in the meantime, but not all data might be available until the backfill is complete.

To get started with evidence finder, see Searching for evidence in evidence finder.

Additional resources

- Troubleshooting evidence finder issues

Disabling evidence finder

If you no longer want to use evidence finder, you can disable the feature at any time.

Follow these steps to learn how to disable evidence finder. Pay close attention to the prerequisites, as you'll need specific permissions to delete the event data store in CloudTrail Lake that was created when you enabled evidence finder.

Prerequisites

Required permissions to disable evidence finder

To disable evidence finder, you need permissions to delete an event data store in CloudTrail Lake. For an example policy that you can use, see Permissions to disable evidence finder.

If you need help with permissions, contact your AWS administrator. If you're an AWS administrator, you can attach the required permission statement to an IAM policy.

Procedure

You can complete this task using the Audit Manager console, the AWS Command Line Interface (AWS CLI), or the Audit Manager API.

> **Warning**
>
> Disabling evidence finder deletes the CloudTrail Lake event data store that Audit Manager created. As a result, you can't re-enable the feature. To re-use evidence finder after you disable it, you must disable AWS Audit Manager, and then re-enable the service completely.

Audit Manager console

To disable evidence finder on the Audit Manager console

1. In the **Evidence finder** section of the Audit Manager settings page, choose **Disable**.
2. In the pop-up window that appears, enter **`Yes`** to confirm your decision.
3. Choose **Request to disable**.

AWS CLI

To disable evidence finder in the AWS CLI

Run the update-settings command with the `--no-evidence-finder-enabled` parameter.

```
aws auditmanager update-settings --no-evidence-finder-enabled
```

Audit Manager API

To disable evidence finder using the API

Call the UpdateSettings operation and use the evidenceFinderEnabled parameter.

For more information, choose the previous links to read more in the *Audit Manager API Reference*. This includes information about how to use this operation and parameter in one of the language-specific AWS SDKs.

Additional resources

- Troubleshooting evidence finder issues

Configuring your default export destination for evidence finder

When you run queries in evidence finder, you can export your search results into a comma-separated values (CSV) file. Use this setting to choose the default S3 bucket where Audit Manager saves your exported files.

Prerequisites

Your S3 bucket must have the required permissions policy to allow CloudTrail to write the export files to it. More specifically, the bucket policy must include an `s3:PutObject` action and the bucket ARN, and list CloudTrail as the service principal.

- For an example permission policy that you can use, see Resource-based policy examples for AWS Audit Manager.
- For instructions to attach this policy to your S3 bucket, see Adding a bucket policy by using the Amazon S3 console.

- For more tips, see configuration tips for your export destination on this page.

Configuration tips for your export destination

To ensure a successful file export, we recommend that you verify the following configurations for your export destination.

AWS Region

The AWS Region of your customer managed key (if you provided one) must match the Region of your assessment. For instructions on how to change your KMS key, see Audit Manager data encryption settings.

Cross-account S3 buckets

Using a cross-account S3 bucket as your export destination isn't supported in the Audit Manager console. It's possible to specify a cross-account bucket using the AWS CLI or one of the AWS SDKs, but for simplicity, we recommend that you not do this. If you do choose to use a cross-account S3 bucket as your export destination, consider the following points.

- By default, S3 objects—such as CSV exports—are owned by the AWS account that uploads the object. You can use the S3 Object Ownership setting to change this default behavior, so that any new objects that are written by accounts with the `bucket-owner-full-control` canned access control list (ACL) automatically become owned by the bucket owner.

  Although it's not a requirement, we recommend that you make the following changes to your cross-account bucket settings. Making these changes ensures that the bucket owner has full control of the exported files that you publish to their bucket.

  - Set the object ownership of the S3 bucket to *bucket owner preferred*, instead of the default *object writer*
  - Add a bucket policy to ensure that objects uploaded to that bucket have the `bucket-owner-full-control` ACL

- To allow Audit Manager to export files to a cross-account S3 bucket, you must add the following S3 bucket policy to your export destination bucket. Replace the *`placeholder text`* with your own information. The `Principal` element in this policy is the user or role that owns the assessment and exports the file. The `Resource` specifies the cross-account S3 bucket where the file is exported to.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow cross account file exports",
            "Effect": "Allow",
            "Principal": {
                "AWS":
 "arn:aws:iam::111122223333:user/AssessmentOwnerUserName"
            },
            "Action": [
                "s3:ListBucket",
                "s3:PutObject",
                "s3:GetObject",
                "s3:GetBucketLocation",
                "s3:PutObjectAcl",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::CROSS-ACCOUNT-BUCKET",
                "arn:aws:s3:::CROSS-ACCOUNT-BUCKET/*"
            ]
        }
    ]
}
```

Procedure

You can update this setting using the Audit Manager console, the AWS Command Line Interface (AWS CLI), or the Audit Manager API.

Audit Manager console

To update your export destination settings on the Audit Manager console

1. From the **Evidence finder** settings tab, go to the **Export destination** section.
2. Choose one of the following options:

   - If you want to remove the current S3 bucket, choose **Remove** to clear your settings.

- If you want to save a default S3 bucket for the first time, proceed to step 3.

3. Specify the S3 bucket that you want to store your exported files in.

   - Choose **Browse S3** to choose from a list of your buckets.
   - Alternatively, you can enter the bucket URI in this format: **`s3://bucketname/prefix`**

   > **Tip**
   >
   > To keep your destination bucket organized, you can create an optional folder for your CSV exports. To do so, append a slash (**`/`**) and a prefix to the value in the **Resource URI** box (for example, **`/evidenceFinderCSVExports`**). Audit Manager then includes this prefix when it adds the CSV file to the bucket, and Amazon S3 generates the path specified by the prefix. For more information about prefixes in Amazon S3, see Organizing objects in the Amazon S3 console in the *Amazon Simple Storage Service* User Guide.

4. When you're done, choose **Save**.

For instructions on how to create an S3 bucket, see Creating a bucket in the *Amazon S3 User Guide*.

AWS CLI

To update your export destination settings in the AWS CLI

Run the update-settings command and use the `--default-export-destination` parameter to specify an S3 bucket.

In the following example, replace the *`placeholder text`* with your own information:

```
aws auditmanager update-settings --default-export-destination
 destinationType=S3,destination=amzn-s3-demo-destination-bucket
```

For instructions on how to create an S3 bucket, see create-bucket in the *AWS CLI Command Reference*.

Audit Manager API

To update your export destination settings using the API

Call the UpdateSettings operation and use the defaultExportDestination parameter to specify an S3 bucket.

For instructions on how to create an S3 bucket, see CreateBucket in the *Amazon S3 API Reference*.

Notifications in AWS Audit Manager

AWS Audit Manager can notify you about user actions through Amazon Simple Notification Service (Amazon SNS).

Audit Manager sends notifications when one of the following events occurs:

- An audit owner delegates a control set for review.
- A delegate submits a reviewed control set back to the audit owner.
- An audit owner completes the review of a control set.

Additional resources

- To configure your notifications in Audit Manager, see Configuring your Audit Manager notifications.
- To find answers to common questions and issues, see Troubleshooting notification issues in the *Troubleshooting* section of this guide.

Troubleshooting common issues in AWS Audit Manager

As you use AWS Audit Manager, you might encounter certain issues or challenges that require troubleshooting. Whether you're facing challenges with setting up assessments, collecting evidence, or any other aspect of the service, you can use this troubleshooting guide to find our recommendations that help you to help you resolve common problems quickly and efficiently.

We encourage you to review the list of topics below, find the one that best matches your scenario, and follow the provided guidance to get back on track. By following the provided troubleshooting steps, you can likely resolve the issue independently and continue leveraging the full capabilities of Audit Manager. However, if your specific issue isn't covered here, or you're unable to resolve it after following the recommended steps, we recommend that you contact Support for further assistance.

Topics

Troubleshooting assessment and evidence collection issues

You can use the information on this page to resolve common assessment and evidence collection issues in Audit Manager.

Evidence collection issues

- My assessment isn't collecting compliance check evidence from AWS Security Hub
- My assessment isn't collecting compliance check evidence from AWS Config
- My assessment isn't collecting user activity evidence from AWS CloudTrail
- My assessment isn't collecting configuration data evidence for an AWS API call
- A common control isn't collecting any automated evidence
- My evidence is generated at different intervals, and I'm not sure how often it's being collected
- I disabled and then re-enabled Audit Manager, and now my pre-existing assessments are no longer collecting evidence
- On my assessment details page, I'm prompted to recreate my assessment
- What's the difference between a data source and an evidence source?

Assessment issues

- My assessment creation failed
- What happens if I remove an in-scope account from my organization?
- I can't see the services in scope for my assessment
- I can't edit the services in scope for my assessment
- What's the difference between a service in scope and a data source type?

I created an assessment but I can't see any evidence yet

If you can't see any evidence, it's likely that you either didn't wait at least 24 hours after you created the assessment or that there's a configuration error.

We recommend that you check the following:

1. Make sure that 24 hours passed since you created the assessment. Automated evidence becomes available 24 hours after you create the assessment.
2. Make sure that you're using Audit Manager in the same AWS Region as the AWS service that you're expecting to see evidence for.
3. If you expect to see compliance check evidence from AWS Config and AWS Security Hub, make sure that both the AWS Config and Security Hub consoles display results for these checks. The AWS Config and Security Hub results should display in the same AWS Region that you use Audit Manager in.

If you still can't see evidence in your assessment and it's not due to one of these issues, check the other potential causes that are described on this page.

My assessment isn’t collecting compliance check evidence from AWS Security Hub

If you don't see compliance check evidence for an AWS Security Hub control, this could be due to one of the following issues.

Missing configuration in AWS Security Hub

This issue can be caused if you missed some configuration steps when you enabled AWS Security Hub.

To fix this issue, make sure that you enabled Security Hub with the required settings for Audit Manager. For instructions, see Enable and set up AWS Security Hub.

A Security Hub control name was entered incorrectly in your `ControlMappingSource`

When you use the Audit Manager API to create a custom control, you can specify a Security Hub control as a data source mapping for evidence collection. To do this, you enter a control ID as the `keywordValue`.

If you don't see compliance check evidence for a Security Hub control, it could be that the `keywordValue` was entered incorrectly in your `ControlMappingSource`. The `keywordValue` is case sensitive. If you enter it incorrectly, Audit Manager might not recognize that rule. As a result, you might not collect compliance check evidence for that control as expected.

To fix this issue, update the custom control and revise the `keywordValue`. The correct format of a Security Hub keyword varies. For accuracy, reference the list of Supported Security Hub controls .

`AuditManagerSecurityHubFindingsReceiver` Amazon EventBridge rule is missing

When you enable Audit Manager, a rule named `AuditManagerSecurityHubFindingsReceiver` is automatically created and enabled in Amazon EventBridge. This rule enables Audit Manager to collect Security Hub findings as evidence.

If this rule isn't listed and enabled in the AWS Region where you use Security Hub, Audit Manager can't collect Security Hub findings for that Region.

To resolve this issue, go to the EventBridge console and confirm that the `AuditManagerSecurityHubFindingsReceiver` rule exists in your AWS account. If the rule doesn't exist, we recommend that you disable Audit Manager and then re-enable the service. If this action doesn't resolve the issue, or if disabling Audit Manager isn't an option, contact Support for assistance.

Service-linked AWS Config rules created by Security Hub

Keep in mind that Audit Manager doesn't collect evidence from the service-linked AWS Config rules that Security Hub creates. This is a specific type of managed AWS Config rule that's enabled and controlled by the Security Hub service. Security Hub creates instances of these service-linked rules in your AWS environment, even if other instances of the same rules already exist. As a result, to prevent evidence duplication, Audit Manager doesn't support evidence collection from the service-linked rules.

I disabled a security control in Security Hub. Does Audit Manager collect compliance check evidence for that security control?

Audit Manager doesn't collect evidence for disabled security controls.

If you set the status of a security control to disabled in Security Hub, no security checks are performed for that control in the current account and Region. As a result, no security findings are available in Security Hub, and no related evidence is collected by Audit Manager.

By respecting the disabled status that you set in Security Hub, Audit Manager ensures that your assessment accurately reflects the active security controls and findings that are relevant to your environment, excluding any controls that you intentionally disabled.

I set the status of a finding to `Suppressed` in Security Hub. Does Audit Manager collect compliance check evidence about that finding?

Audit Manager collects evidence for security controls that have suppressed findings.

If you set the workflow status of a finding to suppressed in Security Hub, this means that you reviewed the finding and do not believe that any action is needed. In Audit Manager, these suppressed findings are collected as evidence and attached to your assessment. The evidence details show the evaluation status of `SUPPRESSED` reported directly from Security Hub.

This approach ensures that your Audit Manager assessment accurately represents the findings from Security Hub, while also providing visibility into any suppressed findings that may require further review or consideration in an audit.

My assessment isn't collecting compliance check evidence from AWS Config

If you don't see compliance check evidence for an AWS Config rule, this could be due to one of the following issues.

The rule identifier was entered incorrectly in your `ControlMappingSource`

When you use the Audit Manager API to create a custom control, you can specify an AWS Config rule as a data source mapping for evidence collection. The `keywordValue` that you specify depends on the type of rule.

If you don't see compliance check evidence for an AWS Config rule, it could be that the `keywordValue` was entered incorrectly in your `ControlMappingSource`. The `keywordValue` is case sensitive. If you enter it incorrectly, Audit Manager might not recognize the rule. As a result, you might not collect compliance check evidence for that rule as intended.

To fix this issue, update the custom control and revise the `keywordValue`.

- For custom rules, make sure that the `keywordValue` has the `Custom_` prefix followed by the custom rule name. The format of the custom rule name may vary. For accuracy, visit the AWS Config console to verify your custom rule names.
- For managed rules, make sure that the `keywordValue` is the rule identifier in `ALL_CAPS_WITH_UNDERSCORES`. For example, `CLOUDWATCH_LOG_GROUP_ENCRYPTED`. For accuracy, reference the list of supported managed rule keywords.

> **Note**
>
> For some managed rules, the rule identifier is different from the rule name. For example, the rule identifier for restricted-ssh is `INCOMING_SSH_DISABLED`. Make sure to use the rule identifier, not the rule name. To find a rule identifier, choose a rule from the list of managed rules and look for its **Identifier** value.

The rule is a service-linked AWS Config rule

You can use managed rules and custom rules as a data source mapping for evidence collection. However, Audit Manager doesn't collect evidence from most service-linked rules.

There are only two types of service-linked rule that Audit Manager collects evidence from:

- Service-linked rules from Conformance Packs
- Service-linked rules from AWS Organizations

Audit Manager doesn't collect evidence from other service-linked rules, specifically any rules with an Amazon Resource Name (ARN) that contains the following prefix: `arn:aws:config:*:*:config-rule/aws-service-rule/...`

The reason that Audit Manager doesn't collect evidence from most service-linked AWS Config rules is to prevent duplicate evidence in your assessments. A service-linked rule is a specific type of managed rule that enables other AWS services to create AWS Config rules in your account. For example, some Security Hub controls use an AWS Config service-linked rule to run security checks. For each Security Hub control that uses a service-linked AWS Config rule, Security Hub creates an instance of the required AWS Config rule in your AWS environment. This happens even if the original rule already exists in your account. Therefore, to avoid collecting the same evidence from the same rule twice, Audit Manager ignores the service-linked rule and doesn't collect evidence from it.

AWS Config isn't enabled

AWS Config must be enabled in your AWS account. After you've set up AWS Config in this way, Audit Manager collects evidence each time the evaluation of an AWS Config rule occurs. Make sure that you enabled AWS Config in your AWS account. For instructions, see Enable and set up AWS Config.

The AWS Config rule evaluated a resource configuration before you set up your assessment

If your AWS Config rule is set up to evaluate configuration changes for a specific resource, you might see a mismatch between the evaluation in AWS Config and the evidence in Audit Manager. This happens if the rule evaluation occurred before you set up the control in your Audit Manager assessment. In this case, Audit Manager doesn't generate evidence until the underlying resource changes state again and triggers a re-evaluation of the rule.

As a workaround, you can navigate to the rule in the AWS Config console and manually re-evaluate the rule. This invokes a new evaluation of all of the resources that pertain to that rule.

My assessment isn't collecting user activity evidence from AWS CloudTrail

When you use the Audit Manager API to create a custom control, you can specify a CloudTrail event name as a data source mapping for evidence collection. To do so, you enter the event name as the `keywordValue`.

If you don't see user activity evidence for a CloudTrail event, it could be that the `keywordValue` was entered incorrectly in your `ControlMappingSource`. The `keywordValue` is case sensitive. If you enter it incorrectly, Audit Manager might not recognize the event name. As a result, you might not collect user activity evidence for that event as intended.

To fix this issue, update the custom control and revise the `keywordValue`. Make sure that the event is written as `serviceprefix_ActionName`. For example, `cloudtrail_StartLogging`. For accuracy, review the AWS service prefix and action names in the Service Authorization Reference.

My assessment isn't collecting configuration data evidence for an AWS API call

When you use the Audit Manager API to create a custom control, you can specify an AWS API call as a data source mapping for evidence collection. To do so, you enter the API call as the `keywordValue`.

If you don't see configuration data evidence for an AWS API call, it could be that the `keywordValue` was entered incorrectly in your `ControlMappingSource`. The `keywordValue` case sensitive. If you enter it incorrectly, Audit Manager might not recognize the API call. As a result, you might not collect configuration data evidence for that API call as intended.

To fix this issue, update the custom control and revise the `keywordValue`. Make sure that the API call is written as `serviceprefix_ActionName`. For example, `iam_ListGroups`. For accuracy, reference the list of AWS API calls supported by AWS Audit Manager.

A common control isn't collecting any automated evidence

When you review a common control, you might see the following message: **This common control doesn't collect automated evidence from core controls**.

This means that no AWS managed evidence sources can currently support this common control. As a result, the **Evidence sources** tab is empty and no core controls are displayed.

When a common control doesn't collect automated evidence, it's referred to as a *manual common control*. Manual common controls typically require the provision of physical records and signatures, or details about events that occur outside of your AWS environment. For this reason, there are often no AWS data sources that can produce evidence to support the control's requirements.

If a common control is manual, you can still use it as an evidence source for a custom control. The only difference is that the common control won't collect any evidence automatically. Instead, you'll need to manually upload your own evidence to support the requirements of the common control.

To add evidence to a manual common control

1. **Create a custom control**
   - Follow the steps to create or edit a custom control.
   - When you specify evidence sources in step 2, choose the manual common control as an evidence source.
2. **Create a custom framework**
   - Follow the steps to create or edit a custom framework.
   - When you specify a control set in step 2, include your new custom control.
3. **Create an assessment**
   - Follow the steps to create an assessment from your custom framework.
   - At this point, the manual common control is now an evidence source in an active assessment control.
4. **Upload manual evidence**
   - Follow the steps to add manual evidence to the control in your assessment.

> **Note**
>
> As more AWS data sources become available in the future, it's possible that AWS might update the common control to include core controls as evidence sources. In this case, if the common control is an evidence source in one or more of your active assessment controls, you'll benefit from these updates automatically. No further set up is needed from your side, and you'll start to collect automated evidence that supports the common control.

My evidence is generated at different intervals, and I'm not sure how often it's being collected

The controls in Audit Manager assessments are mapped to various data sources. Each data source has a different evidence collection frequency. As a result, there's no one-size-fits-all answer for how often evidence is collected. Some data sources evaluate compliance, whereas others only capture resource state and change data without a compliance determination.

The following is a summary of the different data source types and how often they collect evidence.

Data source type	Description	Evidence collection frequency	When this control is active in an assessment
AWS CloudTrail	Tracks a specific user activity.	Continual	Audit Manager filters your CloudTrail logs based on the keyword that you choose. The processed logs are imported as **User activity** evidence.
AWS Security Hub	Captures a snapshot of your resource security posture by reporting findings from Security Hub.	Based on the schedule of the Security Hub check (typicall y around every 12 hours)	Audit Manager retrieves the security finding directly from Security Hub. The finding is imported as **Compliance check** evidence.
AWS Config	Captures a snapshot of your resource security posture by reporting findings from AWS Config.	Based on the settings that are defined in the AWS Config rule	Audit Manager retrieves the rule evaluation directly from AWS Config. The evaluation is imported as **Compliance check** evidence.

Data source type	Description	Evidence collection frequency	When this control is active in an assessment
AWS API calls	Takes a snapshot of your resource configuration directly through an API call to the specified AWS service.	Daily, weekly, or monthly	Audit Manager makes the API call based on the frequency that you specify. The response is imported as **Configuration data** evidence.

Regardless of the evidence collection frequency, new evidence is collected automatically for as long as the assessment is active. For more information, see Evidence collection frequency.

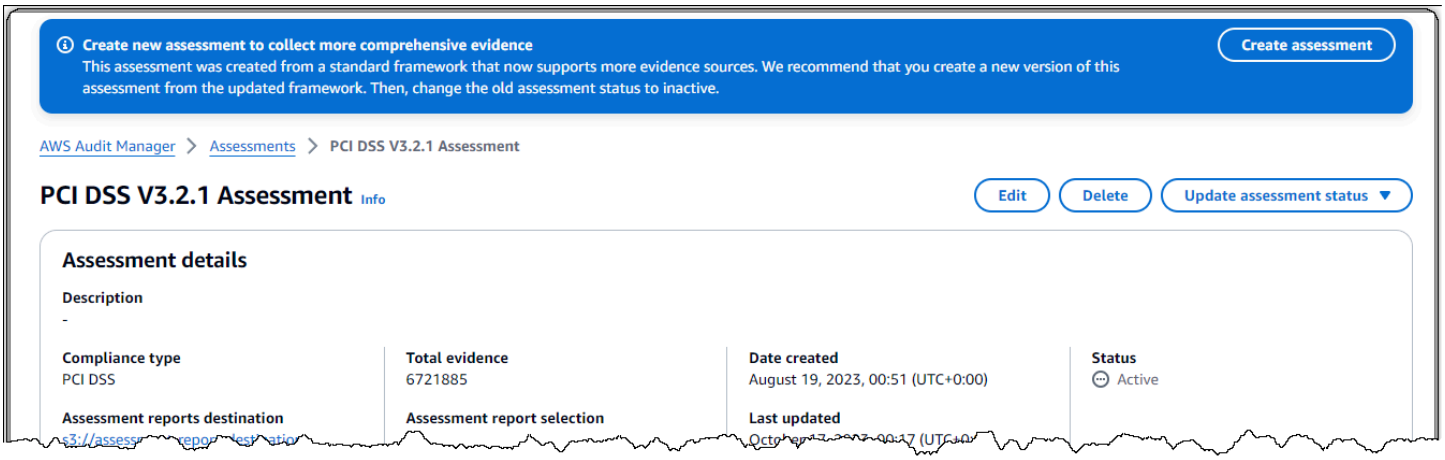
To learn more, see Supported data source types for automated evidence and Changing how often a control collects evidence.

I disabled and then re-enabled Audit Manager, and now my pre-existing assessments are no longer collecting evidence

When you disable Audit Manager and choose not to delete your data, your existing assessments move into a dormant state and stop collecting evidence. This means that when you re-enable Audit Manager, the assessments that you previously created remain available. However, they don't automatically resume evidence collection.

To start collecting evidence again for a pre-existing assessment, edit the assessment and choose **Save** without making any changes.

On my assessment details page, I'm prompted to recreate my assessment



If you see a message that says **Create new assessment to collect more comprehensive evidence**, this indicates that Audit Manager now provides a new definition of the standard framework that your assessment was created from.

In the new framework definition, all of the framework's standard controls can now collect evidence from AWS managed sources. This means that whenever there's an update to the underlying data sources for a common or core control, Audit Manager automatically applies the same update to all related standard controls.

To benefit from these AWS managed sources, we recommend that you create a new assessment from the updated framework. After you do this, you can then change the old assessment status to inactive. This action helps to ensure that your new assessment collects the most accurate and comprehensive evidence that's available from AWS managed sources. If you take no action, your assessment continues to use the old framework and control definitions to collect evidence exactly as it did before.

What's the difference between a data source and an evidence source?

An *evidence source* determines where evidence is collected from. This can be an individual data source, or a predefined grouping of data sources that maps to a core control or a common control.

A *data source* is the most granular type of evidence source. A data source includes the following details that tell Audit Manager where exactly to collect evidence data from:

- Data source type (for example, AWS Config)

- Data source mapping (for example, a specific AWS Config rule such as `s3-bucket-public-write-prohibited`)

My assessment creation failed

If your assessment creation fails, this could be due to one of the following issues.

You selected too many AWS accounts in your assessment scope

If you're using AWS Organizations, Audit Manager can support up to 200 member accounts in the scope of a single assessment. If you exceed this number, the assessment creation will fail.

As a workaround, you can run multiple assessments with different accounts in scope for each assessment up to 250 unique member accounts across all assessments.

An account in your scope is already being assessed by another active assessment

If you try to create an assessment that includes an account that's already in scope for another active assessment, the assessment creation fails. This can happen when multiple teams or organizations are trying to assess the same account simultaneously.

You might see an error message similar to: `Scope: AWS Account [account-id] has assessments in progress`.

To resolve this issue, you can take one of the following actions:

- **Coordinate with other teams** - Contact other teams in your organization to determine which assessments are currently using the account in question. You can then coordinate to avoid overlapping assessment scopes.
- **Modify your assessment scope** - Remove the conflicting account from your assessment scope and create the assessment with the remaining accounts. You can assess the conflicting account separately once the other assessment is complete.
- **Wait for the other assessment to complete** - If the other assessment is temporary or nearing completion, you can wait for it to finish before creating your assessment with the desired scope.

> **Note**
>
> This restriction helps ensure that evidence collection doesn't conflict between multiple assessments and that audit results remain accurate and consistent.

What happens if I remove an in-scope account from my organization?

When an in-scope account is removed from your organization, Audit Manager no longer collects evidence for that account and it will be removed from all assessments where the account is in scope. Removing a member account from all assessments will also reduce the total number of unique accounts in scope, allowing you to add a new account from your organization.

I can't see the services in scope for my assessment

If you don't see the **AWS services** tab, this means that the services in scope are managed for you by Audit Manager. When you create a new assessment, Audit Manager manages the services in scope for you from that point onwards.

If you have an older assessment, it's possible that you saw this tab previously in your assessment. However, Audit Manager automatically removes this tab from your assessment and takes over the management of services in scope when either of the following events occur:

- You edit your assessment
- You edit one of the custom controls that's used in your assessment

Audit Manager infers the services in scope by examining your assessment controls and their data sources, and then mapping this information to the corresponding AWS services. If an underlying data source changes for your assessment, we automatically update the scope as needed to reflect the correct services. This ensures that your assessment collects accurate and comprehensive evidence about all of the relevant services in your AWS environment.

I can't edit the services in scope for my assessment

The Editing an assessment in AWS Audit Manager workflow no longer has an **Edit services** step. This is because Audit Manager now manages which AWS services are in scope for your assessment.

If you have an older assessment, it's possible that you manually defined the services in scope when you created that assessment. However, you can't edit these services moving forward. Audit Manager automatically takes over the management of services in scope for your assessment when either of the following events occur:

- You edit your assessment
- You edit one of the custom controls that's used in your assessment

Audit Manager infers the services in scope by examining your assessment controls and their data sources, and then mapping this information to the corresponding AWS services. If an underlying data source changes for your assessment, we automatically update the scope as needed to reflect the correct services. This ensures that your assessment collects accurate and comprehensive evidence about all of the relevant services in your AWS environment.

What's the difference between a service in scope and a data source type?

A service in scope is an AWS service that's included in the scope of your assessment. When a service is in scope, Audit Manager collects evidence about your usage of that service and its resources.

> **Note**
>
> Audit Manager manages which AWS services are in scope for your assessments. If you have an older assessment, it's possible that you manually specified the services in scope in the past. Moving forward, you can't specify or edit services in scope.

A data source type indicates where exactly the evidence is collected from. If you upload your own evidence, the data source type is *Manual*. If Audit Manager collects the evidence, the data source can be one of four types.

1. AWS Security Hub – Captures a snapshot of your resource security posture by reporting findings from Security Hub.
2. AWS Config – Captures a snapshot of your resource security posture by reporting findings from AWS Config.
3. AWS CloudTrail – Tracks a specific user activity for a resource.
4. AWS API calls – Takes a snapshot of your resource configuration directly through an API call to a specific AWS service.

Here are two examples to illustrate the difference between a service in scope and a data source type.

Example 1

Let's say that you want to collect evidence for a control that's named *4.1.2 - Disallow public write access to S3 buckets*. This control checks the access levels of your S3 bucket policies. For this

control, Audit Manager uses a specific AWS Config rule (s3-bucket-public-write-prohibited) to look for an evaluation of your S3 buckets. In this example, the following is true:

- The service in scope is Amazon S3
- The resources that are being assessed are your S3 buckets
- The data source type is AWS Config
- The data source mapping is a specific AWS Config rule (`s3-bucket-public-write-prohibited`)

Example 2

Let's say that you want to collect evidence for a HIPAA control that's named *164.308(a)(5)(ii)(C)*. This control requires a monitoring procedure for detecting inappropriate sign-ins. For this control, Audit Manager uses CloudTrail logs to look for all AWS Management Console sign-in events. In this example, the following is true:

- The service in scope is IAM
- The resources that are being assessed are your users
- The data source type is CloudTrail
- The data source mapping is a specific CloudTrail event (`ConsoleLogin`)

Troubleshooting assessment report issues

You can use the information on this page to resolve common assessment report issues in Audit Manager.

Topics

- Additional resources

My assessment report failed to generate

Your assessment report might have failed to generate for a number of reasons. You can start to troubleshoot this issue by checking the most frequent causes. Use the following checklist to get started.

1. Check if any of your AWS Region information doesn't match up:
   a. **Does the AWS Region of your customer managed key match the AWS Region of your assessment?**

      If you provided your own KMS key for Audit Manager data encryption, the key must be in the same AWS Region as your assessment. To resolve this issue, change the KMS key to one that's in the same Region as your assessment. For instructions on how to change the KMS key, see Configuring your data encryption settings.

   b. **Does the AWS Region of your customer managed key match the AWS Region of your S3 bucket?**

      If you provided your own KMS key for Audit Manager data encryption, the key must be in the same AWS Region as the S3 bucket that you use as your assessment report destination. To resolve this issue, you can change either the KMS key or the S3 bucket so that they're both in the same Region as your assessment. For instructions on how to change the KMS key, see Configuring your data encryption settings. For instructions on how to change the S3 bucket, see Configuring your default assessment report destination.
2. Check the permissions of the S3 bucket that you're using as the assessment report destination:
   a. **Does the IAM entity that's generating the assessment report have the necessary permissions for the S3 bucket?**

      The IAM entity must have the required S3 bucket permissions to publish reports in that bucket. We provide an example policy that you can use.

   b. **Does the S3 bucket have a bucket policy that requires server-side encryption (SSE) using SSE-KMS?**

      If yes, the KMS key that's used in that bucket policy must match the KMS key that's specified in your Audit Manager data encryption settings. If you didn't configure a KMS key in your Audit Manager settings, and your S3 bucket policy requires SSE, ensure that the bucket policy

allows SSE-S3. For instructions on how to change the KMS key, see Configuring your data encryption settings. For instructions on how to change the S3 bucket, see Configuring your default assessment report destination.

If you're still unable to successfully generate an assessment report, review the following issues on this page.

I followed the checklist above, and my assessment report still failed to generate

Audit Manager limits how much evidence you can add to an assessment report. The limit is based on the AWS Region of your assessment, the Region of the S3 bucket that's used as your assessment report destination, and whether your assessment uses a customer managed AWS KMS key.

1. The limit is 22,000 for same-Region reports (where the S3 bucket and assessment are in the same AWS Region)
2. The limit is 3,500 for cross-Region reports (where the S3 bucket and assessment are in different AWS Regions)
3. The limit is 3,500 if the assessment uses a customer managed KMS key

If you try to generate a report that contains more evidence than this, the operation might fail.

As a workaround, you can generate multiple assessment reports rather than one larger assessment report. By doing this, you can export evidence from your assessment into more manageable-sized batches.

I get an *access denied* error when I try to generate a report

You will get an `access denied` error if your assessment was created by a delegated administrator account that the KMS key that's specified in your Audit Manager settings doesn't belong to. To avoid this error, when you designate a delegated administrator for Audit Manager, make sure that the delegated administrator account has access on the KMS key that you provided when setting up Audit Manager.

You might also receive an `access denied` error if you don't have write permissions for the S3 bucket that you're using as your assessment report destination.

If you get an `access denied` error, make sure that you meet the following requirements:

- Your KMS key in your Audit Manager settings gives permissions to the delegated administrator. You can configure this by following the instructions in Allowing users in other accounts to use a KMS key in the *AWS Key Management Service Developer Guide*. For instructions on how to review and change your encryption settings in Audit Manager, see Configuring your data encryption settings.
- You have a permissions policy that grants you write access for the S3 bucket that you're using as the assessment report destination. More specifically, your permissions policy contains an `s3:PutObject` action, specifies the ARN of the S3 bucket, and includes the KMS key that's used to encrypt your assessment reports. For an example policy that you can use, see Example 2 (Assessment report destination permissions).

> **Note**
>
> If you change your Audit Manager data encryption settings, these changes apply to the new assessments that you create moving forward. This includes any assessment reports that you create from your new assessments.
>
> The changes don't apply to existing assessments that you created before you changed your encryption settings. This includes new assessment reports that you create from existing assessments, in addition to existing assessment reports. Existing assessments—and all their assessment reports—continue to use the old KMS key. If the IAM identity that's generating the assessment report doesn't have permissions to use the old KMS key, you can grant permissions at the key policy level.

I'm unable to unzip the assessment report

If you can't unzip the assessment report on Windows, it's likely that Windows Explorer can't extract it because its file path has several nested folders or long names. This is because, under the Windows file naming system, the folder path, file name, and file extension can't exceed 259 characters. Otherwise, this results in a `Destination Path Too Long` error.

To resolve this issue, try moving the zip file to the parent folder of its current location. You can then try again to unzip it from there. Alternatively, you can also try shortening the name of the zip file or extracting it to a different location that has a shorter file path.

When I choose an evidence name in a report, I'm not redirected to the evidence details

This issue might happen if you're interacting with the assessment report in a browser, or using the default PDF reader that's installed on your operating system. Some browser and system default PDF readers don't allow the opening of relative links. This means that, although hyperlinks might work within the assessment report summary PDF (such as hyperlinked control names in the table of contents), hyperlinks are ignored when you attempt to navigate away from the assessment summary PDF to a separate evidence detail PDF.

If you encounter this issue, we recommend that you use a dedicated PDF reader to interact with your assessment reports. For a reliable experience, we recommend that you install and use Adobe Acrobat Reader, which you can download at the Adobe website. Other PDF readers are also available, but Adobe Acrobat Reader has been proven to work consistently and reliably with Audit Manager assessment reports.

My assessment report generation is stuck in *In progress* status, and I'm not sure how this impacts my billing

Assessment report generation has no impact on billing. You're only billed based on the evidence that your assessments collect. For more information about pricing, see AWS Audit Manager Pricing.

Additional resources

The following pages contain troubleshooting guidance about generating an assessment report from evidence finder:

- I can't generate multiple assessment reports from my search results
- I can't include specific evidence from my search results
- Not all of my evidence finder results are included in the assessment report
- I want to generate an assessment report from my search results, but my query statement is failing

Troubleshooting control and control set issues

You can use the information on this page to resolve common issues with controls in Audit Manager.

General issues

- I can’t see any controls or control sets in my assessment
- I can’t upload manual evidence to a control
- What does it mean if a control says “Replacement available”?

AWS Config integration issues

- I need to use multiple AWS Config rules as a data source for a single control
- The custom rule option is unavailable when I’m configuring a control data source
- The custom rule option is available, but no rules appear in the dropdown list
- Some custom rules are available, but I can’t see the rule that I want to use
- I can’t see the managed rule that I want to use
- I want to share a custom framework, but it has controls that use custom AWS Config rules as a data source. Can the recipient collect evidence for these controls?
- What happens when a custom rule is updated in AWS Config? Do I need to take any action in Audit Manager?

I can’t see any controls or control sets in my assessment

In short, to view the controls for an assessment, you must be specified as an audit owner for that assessment. Moreover, you need the necessary IAM permissions to view and manage the related Audit Manager resources.

If you need access to the controls in an assessment, ask one of the audit owners for that assessment to specify you as audit owner. You can specify audit owners when you're creating or editing an assessment.

Make sure also that you have the necessary permissions to manage the assessment. We recommend that audit owners use the AWSAuditManagerAdministratorAccess policy. If you need help with IAM permissions, contact your administrator or AWS Support. For more information about how to attach a policy to an IAM identity, see Adding Permissions to a User and Adding and removing IAM identity permissions in the *IAM User Guide*.

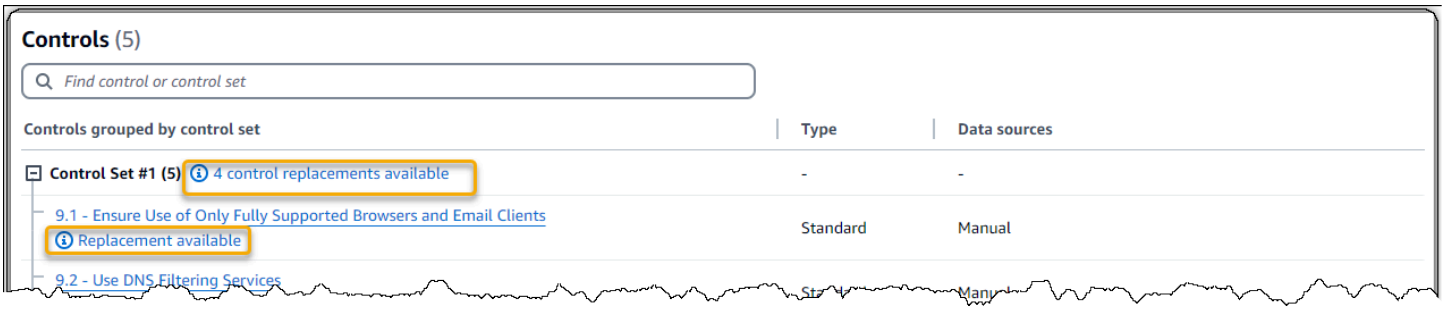
I can’t upload manual evidence to a control

If you can't manually upload evidence to a control, it's likely because the control is in *inactive* status.

To upload manual evidence to a control, you must first change the control status to either *Under review* or *Reviewed*. For instructions, see Changing the status of an assessment control in AWS Audit Manager.

> **Important**
>
> Each AWS account can only manually upload up to 100 evidence files to a control each day. Exceeding this daily quota causes any additional manual uploads to fail for that control. If you need to upload a large amount of manual evidence to a single control, upload your evidence in batches across several days.

What does it mean if a control says “Replacement available”?



If you see this message, this means that an updated control definition is available for one or more of the standard controls in your custom framework. We recommend that you replace these controls so that you can benefit from the improved evidence sources that Audit Manager now provides.

For instructions on how to proceed, see On my custom framework details page, I’m prompted to recreate my custom framework.

I need to use multiple AWS Config rules as a data source for a single control

You can use a combination of managed rules and custom rules for a single control. To do this, define multiple evidence sources for the control, and select your preferred rule type for each one. You can define up to 100 customer managed data sources for a single custom control.

The custom rule option is unavailable when I'm configuring a control data source

This means that you don't have permissions to view custom rules for your AWS account or organization. More specifically, you don't have permissions to perform the DescribeConfigRules operation in the Audit Manager console.

To resolve this issue, contact your AWS administrator for help. If you're an AWS administrator, you can provide permissions for your users or groups by managing your IAM policies.

The custom rule option is available, but no rules appear in the dropdown list

This means that no custom rules are enabled and available for use in your AWS account or organization.

If you don't have any custom rules yet in AWS Config, you can create one. For instructions, see AWS Config custom rules in the *AWS Config Developer Guide*.

If you're expecting to see a custom rule, check the following troubleshooting item.

Some custom rules are available, but I can't see the rule that I want to use

If you can't see the custom rule that you're expecting to find, this could be due to one of the following issues.

Your account is excluded from the rule

It's possible that the delegated administrator account that you're using is excluded from the rule.

Your organization's management account (or one of the AWS Config delegated administrator accounts) can create custom organization rules using the AWS Command Line Interface (AWS CLI). When they do so, they can specify a list of accounts to be excluded from the rule. If your account is on this list, the rule isn't available in Audit Manager.

To resolve this issue, contact your AWS Config administrator for help. If you're an AWS Config administrator, you can update the list of excluded accounts by running the put-organization-config-rule command.

The rule wasn't successfully created and enabled in AWS Config

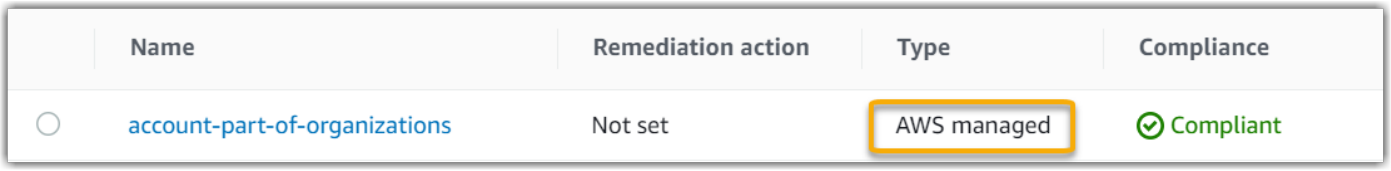
It's also possible that the custom rule wasn't created and enabled successfully. If an error occurred when creating the rule, or the rule isn't enabled, it doesn't appear in the list of available rules in Audit Manager.

For assistance with this issue, we recommend that you contact your AWS Config administrator.

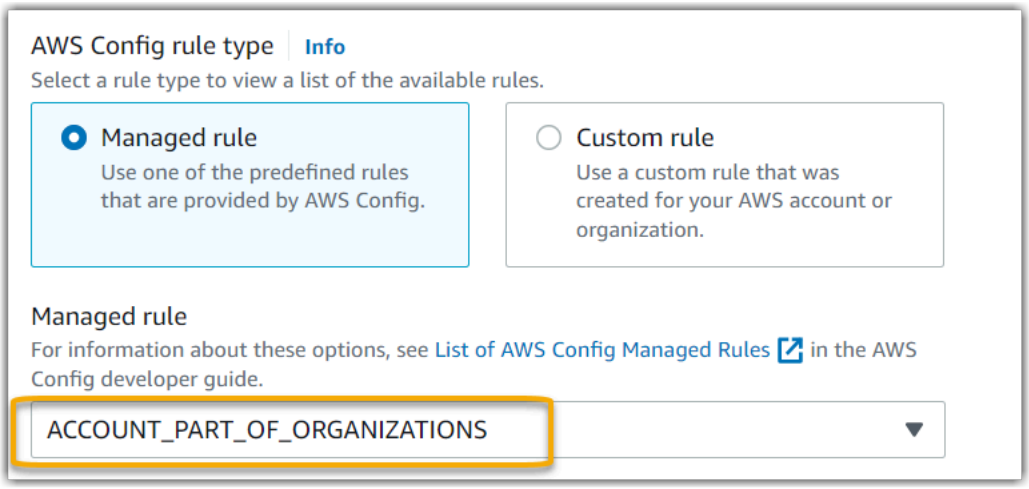
The rule is a managed rule

If you can't find the rule that you're looking for under the dropdown list of custom rules, it's possible that the rule is a managed rule.

You can use the AWS Config console to verify if a rule is a managed rule. To do so, choose **Rules** in the left navigation menu and look for the rule in the table. If the rule is a managed rule, the **Type** column shows **AWS managed**.

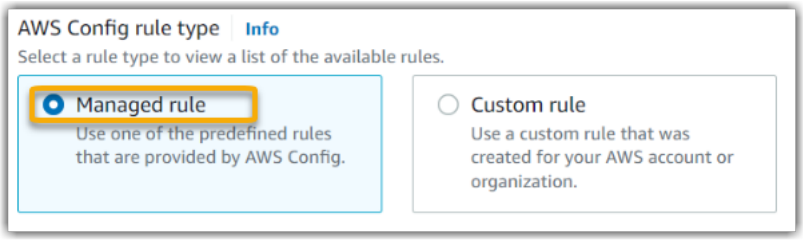


After you've confirmed that it's a managed rule, return to Audit Manager and select **Managed rule** as the rule type. Then, look for the managed rule identifier keyword in the dropdown list of managed rules.



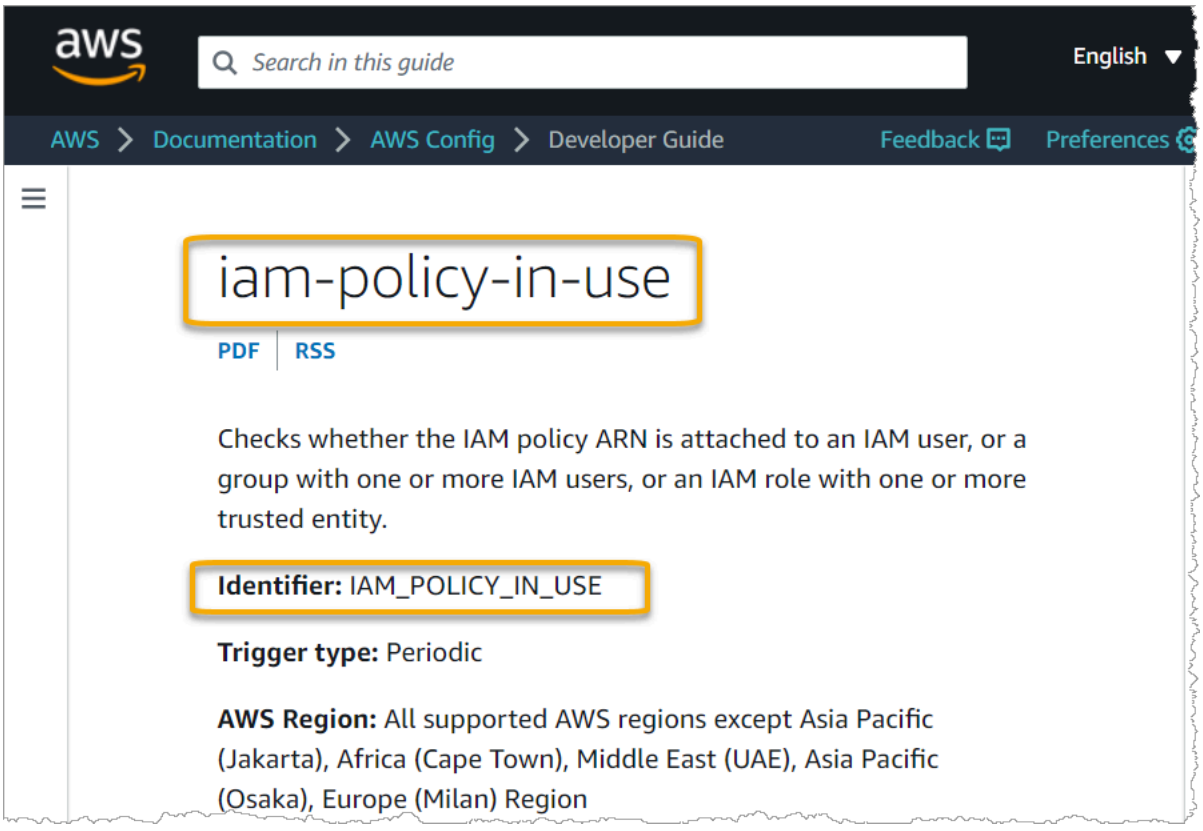
I can't see the managed rule that I want to use

Before you select a rule from the dropdown list in the Audit Manager console, make sure that you selected **Managed rule** as the rule type.



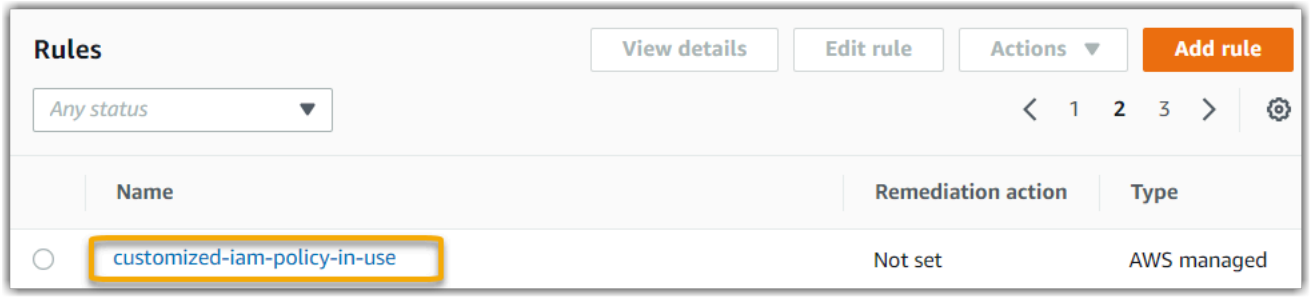
If you still can't see the managed rule that you're expecting to find, it's possible that you're looking for the rule *name*. Instead, you must look for the rule *identifier*.

If you're using a default managed rule, the name and the identifier are similar. The name is in lowercase and uses dashes (for example, `iam-policy-in-use`). The identifier is in uppercase and uses underscores (for example, `IAM_POLICY_IN_USE`). To find the identifier for a default managed rule, review the list of supported AWS Config managed rule keywords and follow the link for the rule that you want to use. This takes you to the AWS Config documentation for that managed rule. From here, you can see both the name and the identifier. Look for the identifier keyword in the Audit Manager dropdown list.

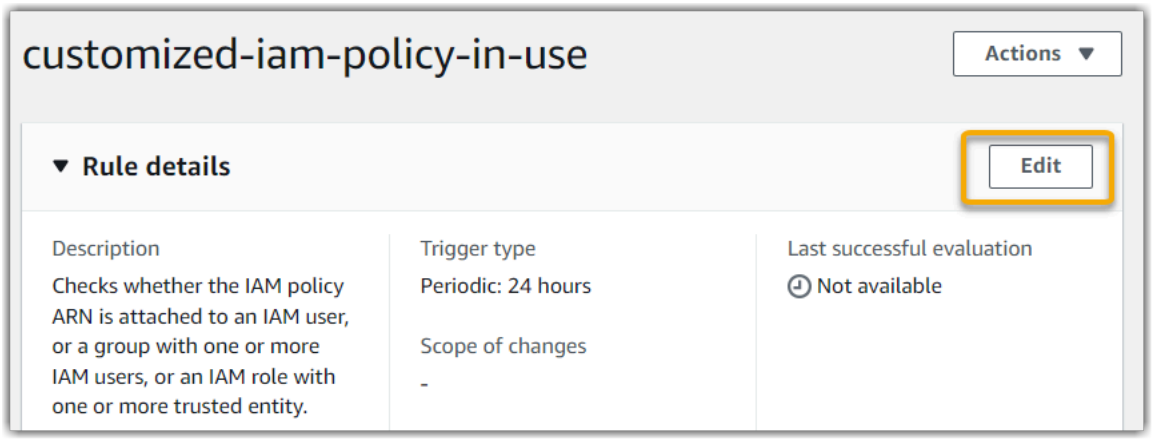


If you're using a custom managed rule, you can use the AWS Config console to find the rule identifier. For example, let's say that you want to use the managed rule called `customized-iam-`

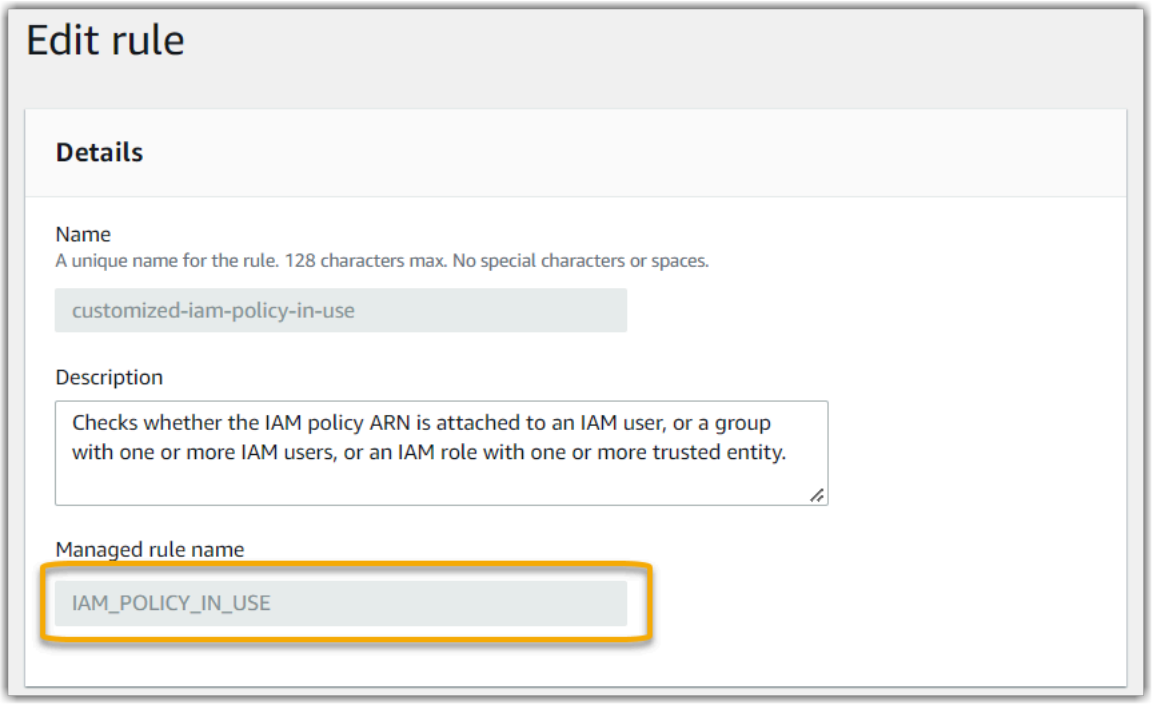
`policy-in-use`. To find the identifier for this rule, go to the AWS Config console, choose **Rules** in the left navigation menu, and choose the rule in the table.



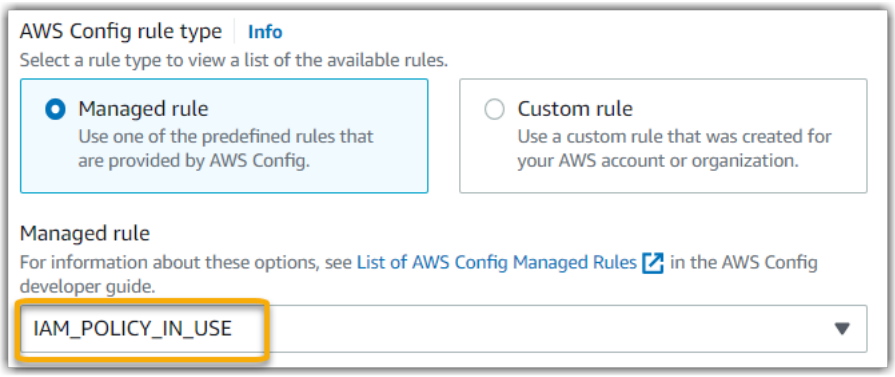
Choose **Edit** to open details about the managed rule.



Under the **Details** section, you can find the source identifier that the managed rule was created from (`IAM_POLICY_IN_USE`).



You can now return to the Audit Manager console and select the same identifier keyword from the dropdown list.



I want to share a custom framework, but it has controls that use custom AWS Config rules as a data source. Can the recipient collect evidence for these controls?

Yes, the recipient can collect evidence for these controls, but a few steps are needed to achieve this.

For Audit Manager to collect evidence using an AWS Config rule as a data source mapping, the following must be true. This applies to both managed rules and custom rules.

1. The rule must exist in the recipient's AWS environment
2. The rule must be enabled in the recipient's AWS environment

Remember that the custom AWS Config rules in your account likely don't exist already in the recipient's AWS environment. Moreover, when the recipient accepts the share request, Audit Manager doesn't recreate any of your custom rules in their account. For the recipient to collect evidence using your custom rules as a data source mapping, they must create the same custom rules in their instance of AWS Config. After the recipient creates and then enables the rules, Audit Manager can collect evidence from that data source.

We recommend that you communicate with the recipient to let them know if any custom rules need to be created in their instance of AWS Config.

What happens when a custom rule is updated in AWS Config? Do I need to take any action in Audit Manager?

For rule updates within your AWS environment

If you update a custom rule within your AWS environment, no action is needed in Audit Manager. Audit Manager detects and handles the rule updates as described in the following table. Audit Manager doesn't notify you when a rule update is detected.

Scenario	What Audit Manager does	What you need to do
A custom rule is **updated** in your instance of AWS Config	Audit Manager continues to report findings for that rule using the updated rule definition.	No action is needed.
A custom rule is **deleted** in your instance of AWS Config	Audit Manager stops reporting findings for the deleted rule.	No action is needed. If you want to, you can edit the custom controls that used the deleted rule as a data source mapping. Doing so helps to clean up your data source settings by removing the deleted rule. Otherwise

Scenario	What Audit Manager does	What you need to do
		, the deleted rule name remains as an unused data source mapping.

For rule updates outside your AWS environment

If a custom rule is updated outside of your AWS environment, Audit Manager doesn't detect the rule update. This is something to consider if you use shared custom frameworks. This is because, in this scenario, the sender and the recipient each work in separate AWS environments. The following table provides recommended actions for this scenario.

Your role	Scenario	Recommended action
Sender	• You shared a framework that uses custom rules as a data source mapping. • After you shared the framework, you updated or deleted one of those rules in AWS Config.	Let the recipient know about your update. That way, they can apply the same update and stay in sync with the latest rule definition.
Recipie	• You accepted a shared framework that uses custom rules as a data source mapping. • After you recreated the custom rules in your instance of AWS Config, the sender updated or deleted one of those rules.	Make the corresponding rule update in your own instance of AWS Config.

Troubleshooting dashboard issues

You can use the information on this page to resolve common dashboard issues in Audit Manager.

Topics

There isn't any data on my dashboard

If the numbers in the Daily snapshot widget display a hyphen (-), this indicates that no data is available. You must have at least one active assessment to see data in the dashboard. To get started, create an assessment. After a 24-hour period, your assessment data will start to appear in the dashboard.

> **Note**
>
> If the numbers in the daily snapshot widget display a zero (0), this indicates that your active assessments (or your selected assessment) have no non-compliant evidence.

The CSV download option isn't available

This option is available for individual assessments only. Make sure that you applied an Assessment filter to the dashboard, then try again. Keep in mind that you can only download one CSV file at a time.

I don't see the downloaded file when trying to download a CSV file

If a control domain contains a large number of controls, there might be a short delay while Audit Manager generates the CSV file. After the file is generated, it downloads automatically.

If you still don’t see the downloaded file, make sure that your internet connection is working normally and you're using the most current version of your web browser. In addition, check your recent downloads folder. Files download into the default location that's determined by your browser. If this doesn't resolve your issue, try downloading the file using a different browser.

A specific control or control domain is missing from the dashboard

This likely means that your active assessments (or specified assessment) don't have any relevant data for that control or control domain.

A control domain is displayed on the dashboard only if both of the following two criteria are met:

- Your active assessments (or specified assessment) contain at least one control that's related to that domain
- At least one control within that domain collected evidence on the date at the top of the dashboard

A control is displayed within a domain only if it collected evidence on the date at the top of the dashboard.

I see similar or duplicate controls appearing under the same control domain

This issue can occur if your assessments collect evidence from different versions of the same standard control.

This happens in the following scenarios:

Scenario 1: You have two assessments created from the same standard framework

- You created an assessment from a standard framework before the launch of the common controls library.

  This assessment collects evidence using outdated standard controls.
- You also created an assessment from the same standard framework after the launch of the common controls library.

  This assessment collects evidence using the new versions of the standard controls.
- As a result, your assessments collect evidence from different versions of the same standard controls.

Scenario 2: You have two assessments created from a custom framework that uses standard controls

- You created an assessment from your custom framework before the launch of the common controls library.

  This assessment collects evidence using outdated standard controls.

- You also created an assessment from the same custom framework after the launch of the common controls library.

  This assessment collects evidence using the new versions of the standard controls.
- As a result, your assessments collect evidence from different versions of the same standard controls.

Example: Let's say you have a pre-existing assessment that you created from the PCI DSS standard framework before June 6th, 2024. Additionally, you created a new assessment from the PCI DSS standard framework after June 6th, 2024. As a result, the first assessment collects evidence using the outdated version of the standard controls for PCI DSS. The second assessment collects evidence using the new version of the standard controls for PCI DSS. Because both versions of the PCI DSS controls are actively collecting evidence in your assessments, you'll likely see both of sets of controls appear in the dashboard under the same control domain. However, in rare cases, the outdated control and the new control might appear under different control domains on the dashboard.

You can continue to collect evidence and view dashboard insights for outdated standard controls and frameworks. However, we encourage you to use the new controls and frameworks that Audit Manager provides following the launch of the common controls library on June 6, 2024. The new standard controls can collect evidence from AWS managed sources. This means that whenever there's an update to the underlying data sources for a common or core control, Audit Manager automatically applies the same update to all related standard controls.

The daily snapshot shows varying amounts of evidence each day. Is this normal?

Not all evidence is collected on a daily basis. The controls in Audit Manager assessments are mapped to different data sources, and each one can have a different evidence collection schedule. As a result, it's expected that the daily snapshot displays a varying amount of evidence each day. For more information, see Evidence collection frequency.

Troubleshooting delegated administrator and AWS Organizations issues

You can use the information on this page to resolve common delegated administrator issues in Audit Manager.

Topics

I can't set up Audit Manager with my delegated administrator account

Although multiple delegated administrators are supported in AWS Organizations, Audit Manager allows only one delegated administrator. If you attempt to designate multiple delegated administrators in Audit Manager, you receive the following error message:

- Console: `You have exceeded the allowed number of delegated administrators for the delegated service`
- CLI: `An error occurred (ValidationException) when calling the RegisterAccount operation: Cannot change delegated Admin for an active account 11111111111 from 2222222222222 to 333333333333`

Choose the one individual account that you want to use as your delegated administrator in Audit Manager. Make sure that you register the delegated administrator account in Organizations first, and then add the same account as a delegated administrator in Audit Manager.

When I create an assessment, I can't see the accounts from my organization under *Accounts in scope*

If you want your Audit Manager assessment to include multiple accounts from your organization, you must specify a delegated administrator.

Make sure that you configured a delegated administrator account for Audit Manager. For instructions, see Adding a delegated administrator.

Some issues to keep in mind:

- You can't use your AWS Organizations management account as a delegated administrator in Audit Manager.
- If you want to enable Audit Manager in more than one AWS Region, you must designate a delegated administrator account separately in each Region. In your Audit Manager settings, designate the same delegated administrator account across all Regions.
- When you designate a delegated administrator, make sure that the delegated administrator account has access on the KMS key that you provide when setting up Audit Manager. To learn how to review and change your encryption settings, see Configuring your data encryption settings.

I get an *access denied* error when I try to generate an assessment report using my delegated administrator account

You will get an `access denied` error if your assessment was created by a delegated administrator account that the KMS key that's specified in your Audit Manager settings doesn't belong to. To avoid this error, when you designate a delegated administrator for Audit Manager, make sure that the delegated administrator account has access on the KMS key that you provided when setting up Audit Manager.

You might also receive an `access denied` error if you don't have write permissions for the S3 bucket that you're using as your assessment report destination.

If you get an `access denied` error, make sure that you meet the following requirements:

- Your KMS key in your Audit Manager settings gives permissions to the delegated administrator. You can configure this by following the instructions in Allowing users in other accounts to use a KMS key in the *AWS Key Management Service Developer Guide.* For instructions on how to review and change your encryption settings in Audit Manager, see Configuring your data encryption settings.
- You have a permissions policy that grants you write access for the assessment report destination. More specifically, your permissions policy contains an `s3:PutObject` action, specifies the ARN

of the S3 bucket, and includes the KMS key that's used to encrypt your assessment reports. For an example policy that you can use, see Example 2 (Assessment report destination permissions).

> **Note**
>
> If you change your Audit Manager data encryption settings, these changes apply to the new assessments that you create moving forward. This includes any assessment reports that you create from your new assessments.
>
> The changes don't apply to existing assessments that you created before you changed your encryption settings. This includes new assessment reports that you create from existing assessments, in addition to existing assessment reports. Existing assessments—and all their assessment reports—continue to use the old KMS key. If the IAM identity that's generating the assessment report doesn't have permissions to use the old KMS key, you can grant permissions at the key policy level.

What happens in Audit Manager if I unlink a member account from my organization?

When you unlink a member account from an organization, Audit Manager receives a notification about this event. Audit Manager then automatically removes that AWS account from the *accounts in scope* lists of your existing assessments. When you specify the scope of new assessments moving forward, the unlinked account no longer appears in the list of eligible AWS accounts.

When Audit Manager removes an unlinked member account from the *accounts in scope* lists of your assessments, you aren't notified of this change. Moreover, the unlinked member account isn't notified that Audit Manager is no longer enabled on their account.

What happens if I relink a member account to my organization?

When you relink a member account to your organization, that account isn't automatically added to the scope of your existing Audit Manager assessments. However, the relinked member account now appears as an eligible AWS account when you specify the *accounts in scope* of your assessments.

- For existing assessments, you can manually edit the assessment scope to add the relinked member account. For instructions, see Step 2: Edit AWS accounts in scope.

- For new assessments, you can add the relinked account during assessment setup. For instructions, see Step 2: Specify AWS accounts in scope.

What happens if I migrate a member account from one organization to another?

If a member account has Audit Manager enabled in organization 1 and then migrates to organization 2, Audit Manager is not enabled for organization 2 as a result.

Troubleshooting evidence finder issues

Use the information on this page to resolve common evidence finder issues in Audit Manager.

General evidence finder issues

- I can't enable evidence finder
- I enabled evidence finder, but I don't see past evidence in my search results
- I can't disable evidence finder
- My search query fails
- I see that a control domain is marked as “outdated”. What does this mean?

Evidence finder assessment report issues

- I can’t generate multiple assessment reports from my search results
- I can't include specific evidence from my search results
- Not all of my evidence finder results are included in the assessment report
- I want to generate an assessment report from my search results, but my query statement is failing
- Additional resources

Evidence finder CSV export issues

- My CSV export failed

- I can't export specific evidence from my search results
- I can’t export multiple CSV files at once

I can't enable evidence finder

Common reasons why you can't enable evidence finder include the following situations:

You're missing permissions

If you’re trying to enable evidence finder for the first time, make sure that you have the required permissions to enable evidence finder. These permissions allow you to create and manage an event data store in CloudTrail Lake, which is necessary to support evidence finder search queries. The permissions also allow you to run search queries in evidence finder.

If you need help with permissions, contact your AWS administrator. If you’re an AWS administrator, you can copy the required permission statement and attach it to an IAM policy.

You're using your Organizations management account

Keep in mind that you can't use your management account to enable evidence finder. Sign in as the delegated administrator account, and try again.

You previously disabled evidence finder

Re-enabling evidence finder isn't currently supported. If you previously disabled evidence finder, you can't enable it again.

I enabled evidence finder, but I don't see past evidence in my search results

When you enable evidence finder, it takes up to 7 days for all of your past evidence data to become available.

During this 7-day period, an event data store is backfilled with your past two years’ worth of evidence data. This means that if you use evidence finder immediately after you enable it, not all results are available until the backfill is complete.

For instructions on how to check the status of the data backfill, see Confirming the status of evidence finder.

I can't disable evidence finder

This could be caused by one of the following reasons.

You're missing permissions

If you're trying to disable evidence finder, make sure that you have the required permissions to disable evidence finder. These permissions allow you to update and delete an event data store in CloudTrail Lake, which is necessary to disable evidence finder.

If you need help with permissions, contact your AWS administrator. If you're an AWS administrator, you can copy the required permission statement and attach it to an IAM policy.

A request to enable evidence finder is still in progress

When you request to enable evidence finder, we create an event data store to support evidence finder queries. You can't disable evidence finder while the event data store is being created.

To proceed, wait until the event data store is created, and try again. For more information, see Confirming the status of evidence finder.

You already requested to disable evidence finder

When you request to disable evidence finder, we delete the event data store that's used for evidence finder queries. If you try again to disable evidence finder while the event data store is being deleted, you get an error message.

In this case, no action is needed. Wait for the event data store to be deleted. As soon as this is complete, evidence finder is disabled. For more information, see Confirming the status of evidence finder.

My search query fails

A failed search query could be caused by one of the following reasons.

You're missing permissions

Verify that the user has the required permissions to run search queries and access the search results. Specifically, you need permissions for the following CloudTrail actions:

- StartQuery
- DescribeQuery

- CancelQuery
- GetQueryResults

If you need help with permissions, contact your AWS administrator. If you're an AWS administrator, you can copy the required permission statement and attach it to an IAM policy.

You're running the maximum number of queries

You can run up to 5 queries at a time. If you're running the maximum number of concurrent queries, this results in a `MaxConcurrentQueriesException` error. If you get this error message, wait a minute for some queries to finish, and then run the query again.

Your query statement has a validation error

If you're using the API or CLI to perform the CloudTrail Lake StartQuery operation, make sure that your `queryStatement` is valid. If the query statement has validation errors, incorrect syntax, or unsupported keywords, this results in an `InvalidQueryStatementException`.

For more information about writing a query, see Create or edit a query in the *AWS CloudTrail User Guide*.

For examples of valid syntax, review the following query statement examples that can be used to query an Audit Manager event data store.

Example 1: Investigate evidence and its compliance status

This example finds evidence with any compliance status across all assessments in account, within a specified date range.

```
SELECT eventData.evidenceId, eventData.resourceArn,
 eventData.resourceComplianceCheck FROM $EDS_ID WHERE eventTime > '2022-11-02
 00:00:00.000' AND eventTime < '2022-11-03 00:00:00.000'
```

Example 2: Determine non-compliant evidence for a control

This example finds all non-compliant evidence in a specified date range for a specific assessment and control.

```
SELECT * FROM $EDS_ID WHERE eventData.assessmentId = '11aa33bb-55cc-77dd-99ee-
ff22gg44hh66' AND eventTime > '2022-10-27 22:05:00.000' AND eventTime
 < '2022-11-03 22:05:00.000' AND eventData.resourceComplianceCheck IN
 ('NON_COMPLIANT','FAILED','WARNING') AND eventData.controlId IN ('aa11bb22-cc33-
dd44-ee55-ff66gg77hh88')
```

Example 3: Count evidence by name

This example lists the total evidence for an assessment in a specified date range, grouped by name and ordered by evidence count.

```
SELECT eventData.eventName as eventName, COUNT(*) as totalEvidence FROM  $EDS_ID
 WHERE eventData.assessmentId = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' AND eventTime
 > '2022-10-27 22:05:00.000' AND eventTime < '2022-11-03 22:05:00.000' GROUP BY
 eventData.eventName ORDER BY totalEvidence DESC
```

Example 4: Explore evidence by data source and service

This example finds all evidence in a specified date range for a specific data source and service.

```
SELECT * FROM $EDS_ID WHERE eventTime > '2022-10-27 22:05:00.000' AND eventTime
 < '2022-11-03 22:05:00.000' AND eventData.service IN ('dynamodb') AND
 eventData.dataSource IN ('AWS API calls')
```

Example 5: Explore compliant evidence by data source and control domain

This example finds compliant evidence for specific control domains, where the evidence comes from a data source that isn't AWS Config.

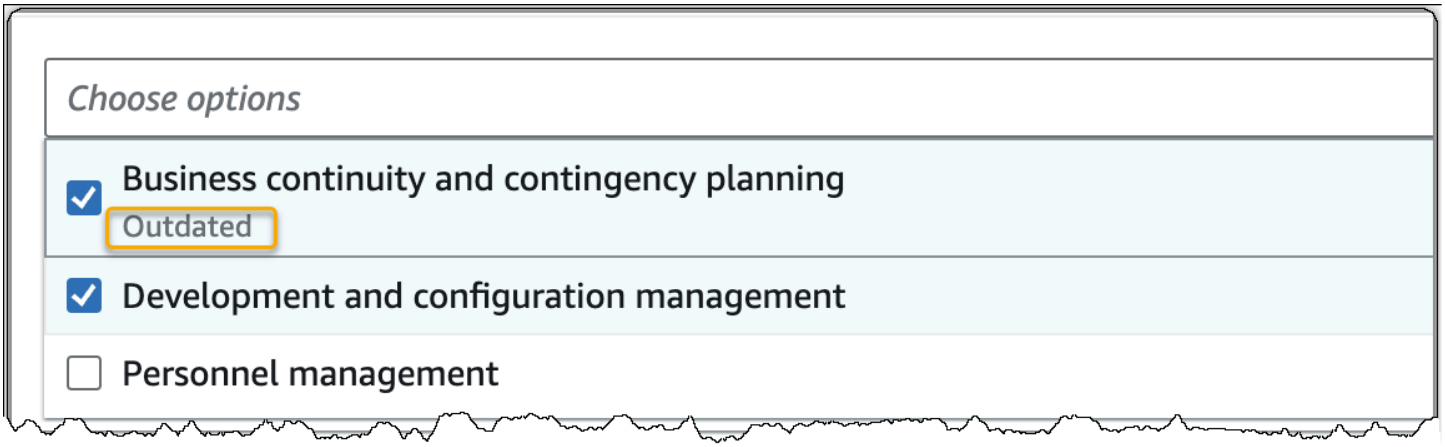
```
 SELECT * FROM $EDS_ID WHERE eventData.resourceComplianceCheck IN
 ('PASSED','COMPLIANT') AND eventData.controlDomainName IN ('Logging and
 monitoring','Data security and privacy') AND eventData.dataSource NOT IN ('AWS
 Config')
```

Other API exceptions

The StartQuery API might fail for several other reasons. For a complete list of possible errors and descriptions, see StartQuery Errors in the *AWS CloudTrail API Reference.*

I see that a control domain is marked as “outdated”. What does this mean?

When you apply a control domain filter in evidence finder, you might notice that some available control domains are described as **Outdated**.



As of June 6, 2024, Audit Manager supports a new set of control domains provided by AWS Control Catalog. To fetch a list of these control domains, see ListDomains in the *AWS Control Catalog API Reference*.

If a control domain is marked as **Outdated**, this means that the control domain you're viewing isn't one of the new control domains provided by AWS Control Catalog. Audit Manager continues to support these outdated control domains so that you can still use them as criteria when you search for evidence.

Although we continue to support the outdated control domains, we encourage you to use the new control domains instead. The new control domains are mapped to the updated standard controls that were launched as part of the common controls library on June 6, 2024. On this date, we released updated standard controls that can collect evidence from AWS managed sources. This means that whenever there's an update to the underlying data sources for a common or core control, Audit Manager automatically applies the same update to all related standard controls.

I can't generate multiple assessment reports from my search results

This error is caused by running too many CloudTrail Lake queries at the same time.

This error can happen if you group your search results and attempt to immediately generate assessment reports for each line item in your grouped results. When you get your search results and generate an assessment report, each action invokes a query. You can only run up to 5 queries at one time. If you're running the maximum number of concurrent queries, a `MaxConcurrentQueriesException` error is returned.

To prevent this error, make sure that you aren't generating too many assessment reports at one time. If you're running the maximum number of concurrent queries, a

`MaxConcurrentQueriesException` error is returned. If you get this error message, wait a few minutes for your in-progress assessment reports to complete.

You can check the status of your assessment reports from the download center page in the Audit Manager console. After your reports are complete, return to your grouped results in evidence finder. You can then continue to get the results and generate an assessment report for each line item.

I can't include specific evidence from my search results

All of your search results are included in the assessment report. You can't selectively add individual rows from your set of search results.

If you only want to include specific search results in the assessment report, we recommend that you edit your current search filters. This way, you can narrow down your results to target only the evidence that you want to include in the report.

Not all of my evidence finder results are included in the assessment report

When you generate an assessment report, there are limits for how much evidence you can add. The limit is based on the AWS Region of your assessment, the Region of the S3 bucket that's used as your assessment report destination, and whether your assessment uses a customer managed AWS KMS key.

1. The limit is 22,000 for same-Region reports (where the S3 bucket and assessment are in the same AWS Region)
2. The limit is 3,500 for cross-Region reports (where the S3 bucket and assessment are in different AWS Regions)
3. The limit is 3,500 if the assessment uses a customer managed KMS key

If you exceed this limit, the report is still created. However, Audit Manager adds only the first 3,500 or 22,000 evidence items to the report.

To prevent this issue, we recommend that you edit your current search filters. This way, you can reduce your search results by targeting a smaller amount of evidence. If needed, you can repeat this method and generate multiple assessment reports instead of one larger report.

I want to generate an assessment report from my search results, but my query statement is failing

If you're using the CreateAssessmentReport API and your query statement returns a validation exception, check the table below for guidance on how to fix it.

> **Note**
>
> Even if a query statement works in CloudTrail, the same query might not be valid for assessment report generation in Audit Manager. This is because of some differences in query validation between the two services.

Clause	Issue	Solution	Notes
`SELECT`	The `SELECT` clause contains a column name	Remove the `SELECT` clause and replace with `SELECT eventJson .`	Only `SELECT eventJson` is supported. This validation is handled by Audit Manager.
`FROM`	The `FROM` clause contains an invalid event data store ID or The provided event data store ID doesn't match the event data store ID in your Audit Manager settings	Remove the `FROM` clause and replace with `FROM edsID`, where the value of `edsID` matches the event data store ID that's specified in your Audit Manager settings. You can retrieve the ARN of the event data store from your Audit Manager settings. For more information, see GetSettings in the *AWS Audit Manager API Reference*.	This validation is handled by Audit Manager.

Clause	Issue	Solution	Notes
GROUP BY	A GROUP BY clause is present in the query	Remove the GROUP BY clause.	This validation is handled by Audit Manager.
HAVING	A HAVING clause is present in the query	Remove the HAVING clause.	This validation is handled by Audit Manager.
LIMIT	The LIMIT clause contains a value that exceeds the maximum allowed limit	If the LIMIT clause exists, ensure that its value is equal to or less than the maximum supported limit: • For same-Region reports, the limit is 22,000 • For cross-Region reports, the limit is 3,500 • For reports where the related assessment uses a customer managed AWS KMS key, the limit is 3,500	In the console, there's no limit to the number of evidence results that can be returned. However, when generating an assessment report, a limit applies to the amount of evidence that you can include. If no LIMIT value is provided in your query statement, the default maximum limits are applied. This validation is handled by Audit Manager.
ORDER BY	The ORDER BY clause contains Aggregate functions or Aliases that aren't present in the SELECT clause	Ensure that the ORDER BY clause doesn't contain any conditions using Aggregate functions or Aliases.	This validation is handled by the CloudTrail StartQuery API.

Clause	Issue	Solution	Notes
WHERE	The WHERE clause contains more than one assessmentId or The WHERE clause contains an assessmentId that doesn't match the assessmentId in your createAssessmentReport request or The WHERE clause contains an unsupported column name	Ensure that only one assessmentID is specified, and that it matches the assessmentId parameter that you specified in the createAssessmentReport API request. Remove any unsupported column names.	This validation is handled by the CloudTrail StartQuery API.

Examples

The following examples show how you can use the queryStatement parameter when calling the CreateAssessmentReport operation. Before you use these queries, replace the *placeholder text* with your own edsId and assessmentId values.

Example 1: Create a report (same-Region limit applies)

This example creates a report that includes results for S3 buckets created between January 22-23rd, 2022.

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' AND eventTime > '2022-01-22 00:00:00.000' AND
 eventTime < '2022-01-23 00:00:00.000' AND eventName='CreateBucket' LIMIT 22000
```

Example 2: Create a report (cross-Region limit applies)

This example creates a report that includes all results for the specified event data store and assessment, with no date range specified.

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' LIMIT 7000
```

Example 3: Create a report (under the default limit)

This example creates a report that includes all results for the specified event data store and assessment, with a limit that's under the default maximum.

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' LIMIT 2000
```

Additional resources

The following page contains general troubleshooting guidance about assessment reports:

- Troubleshooting assessment report issues

My CSV export failed

Your CSV export might fail for a number of reasons. You can troubleshoot this issue by checking the most frequent causes.

First, make sure that you meet the prerequisites for using the CSV export feature:

You successfully enabled evidence finder

If you haven't enabled evidence finder, you can't run a search query and export your search results.

The backfill of your event data store is complete

If you use evidence finder immediately after you enable it, and the evidence backfill is still in progress, there may be some results that aren't available. To check the backfill status, see Confirming the status of evidence finder.

Your search query succeeded

Audit Manager can't export the results of a failed query. To troubleshoot a failed query, see My search query fails.

After you've confirmed that you meet the prerequisites, use the following checklist to check for potential issues:

1. Check the status of your search query:
   a. **Was the query cancelled?** Evidence finder displays partial results that were processed before the query was cancelled. However, Audit Manager doesn't export partial results to your S3 bucket or the download center.
   b. **Has the query been running for over one hour?** Queries that run for longer than one hour might time out. Evidence finder displays partial results that were processed before the query timed out. However, Audit Manager doesn't export partial results. To avoid a timeout, you can reduce the amount of evidence that's scanned by Editing search filters to specify a narrower time range.
2. Check the name and the URI of your export destination S3 bucket:
   a. **Does the bucket that you specified exist?** If you manually entered a bucket URI, make sure that you didn't mistype anything. A typo or an incorrect URI can result in a `RESOURCE_NOT_FOUND` error when Audit Manager attempts to export the CSV file to Amazon S3.
3. Check the permissions of your export destination S3 bucket:
   a. **Do you have write permissions for the S3 bucket?** You must have write access for the S3 bucket that you're using as the export destination. More specifically, the IAM permissions policy must include an `s3:PutObject` action and the bucket ARN, and list CloudTrail as the service principal. We provide an example policy that you can use.
4. Check if any of your AWS Region information doesn't match up:
   a. **Does the AWS Region of your customer managed key match the AWS Region of your assessment?** If you provided a customer managed key for data encryption, it must be in the

same AWS Region as your assessment. For instructions on how to change the KMS key, see Configuring your data encryption settings.

5. Check the permissions of your delegated administrator account:

   a. **Does the customer managed key in your Audit Manager settings grant permissions to your delegated administrator?** If you're using a delegated administrator account and you specified a customer managed key for data encryption, make sure the delegated administrator has access on that KMS key. For instructions, see Allowing users in other accounts to use a KMS key in the *AWS Key Management Service Developer Guide.* To review and change your encryption settings in Audit Manager, see Configuring your data encryption settings.

> **Note**
>
> If you change your Audit Manager data encryption settings, these changes apply to new assessments that you create moving forward. This includes any CSV files that you export from your new assessments.
>
> The changes don't apply to existing assessments that you created before you changed your encryption settings. This includes new CSV exports from existing assessments, in addition to existing CSV exports. Existing assessments—and all their CSV exports—continue to use the old KMS key. If the IAM identity that's exporting the CSV file doesn't have permissions to use the old KMS key, you can grant permissions at the key policy level.

I can't export specific evidence from my search results

All of your search results are included in the results.

If you want to include only specific evidence in the CSV file, we recommend that you edit your current search filters. This way, you can narrow your results to target only the evidence that you want to export.

I can't export multiple CSV files at once

This error is caused by running too many CloudTrail Lake queries at the same time.

This can happen if you group your search results and attempt to immediately export a CSV file for each line item in your grouped results. When you get your search results and export a CSV file, each of these actions invokes a query. You can run only up to five queries at one time. If you're

running the maximum number of concurrent queries, a `MaxConcurrentQueriesException` error is returned.

To prevent this error, make sure that you aren't exporting too many CSV files at one time.

To resolve this error, wait for your in-progress CSV exports to complete. Most exports take a few minutes. However, if you're exporting a very large amount of data, it might take up to an hour to complete the export. Feel free to navigate away from evidence finder while the export is in progress.

You can check the export status from the download center in the Audit Manager console. After your exported files are ready, return to your grouped results in evidence finder. You can then continue to get the results and export a CSV file for each line item.

Troubleshooting framework issues

You can use the information on this page to resolve common framework issues in Audit Manager.

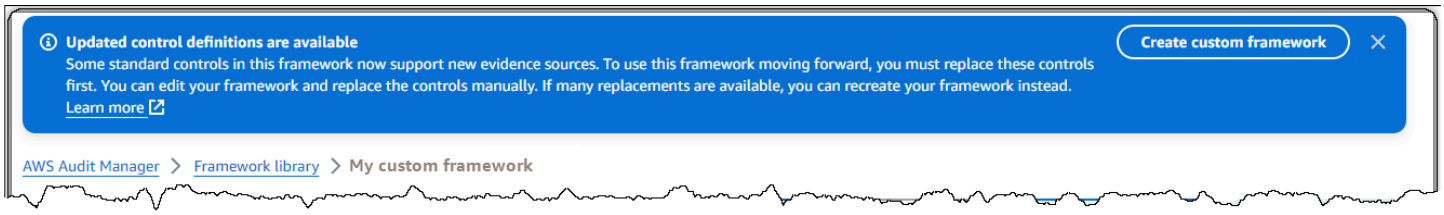
General framework issues

- On my custom framework details page, I'm prompted to recreate my custom framework
- I can't make a copy of my custom framework

Framework sharing issues

- My sent share request status displays as *Failed*
- My share request has a blue dot next to it. What does this mean?
- My shared framework has controls that use custom AWS Config rules as a data source. Can the recipient collect evidence for these controls?
- I updated a custom rule that's used in a shared framework. Do I need to take any action?

On my custom framework details page, I'm prompted to recreate my custom framework



If you see a message that says **Updated control definitions are available**, this indicates that Audit Manager now provides newer definitions for some of the standard controls that are in your custom framework.

Standard controls can now collect evidence from AWS managed source. This means that whenever Audit Manager updates the underlying data sources for a common or core control, the same update is automatically applied to the related standard controls. This helps you to ensure continuous compliance as the cloud compliance environment changes. To make sure that you benefit from these AWS managed sources, we recommend that you replace the controls in your custom framework.

In your custom framework, Audit Manager indicates which controls have replacements available. You'll need to replace these controls before you can make a copy of your custom framework. The next time that you edit your custom framework, we'll prompt you to replace these controls along with any other edits you'd like to make.

There are two ways to replace the controls in your custom framework:

1. Recreate your custom framework

If a large number of controls have replacements available, we recommend that you recreate your custom framework. This is likely to be the best option if your custom framework is based on a standard framework.

- For example, let's say you created your custom framework using NIST SP 800-53 Rev 5 as the starting point. This standard framework has 1007 standard controls, and you added 20 custom controls.
- In this case, the most efficient option is to find `NIST 800-53 (Rev. 5) Low-Moderate-High` in the framework library and make an editable copy of that framework. During this process, you can add the same 20 custom controls that you used before. Because you're now using the

latest definition of the standard framework as your starting point, your custom framework automatically inherits the latest definitions for all of the 1007 standard controls.

2. Edit your custom framework

If a small number of controls have replacements available, we recommend that you edit your custom framework and replace the controls manually.

- For example, let's say you created your custom framework from scratch. In your custom framework, you added 20 custom controls that you created yourself, and eight standard controls from the ACSC Essential Eight standard framework.
- In this case, because a maximum of eight controls would have updates available, the most efficient option is to edit your custom framework and replace those controls one by one. For instructions, see the following procedure.

To manually replace controls in your custom framework

To manually replace controls in your custom framework

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. In the left navigation pane, choose **Framework library**, then choose the **Custom frameworks** tab.
3. Select the framework that you want to edit, choose **Actions**, and then choose **Edit**.
4. On the **Edit framework details** page, choose **Next**.
5. On the **Edit control sets** page, review the name of each control set to see if any of its controls have replacements available.
6. Choose an affected control set to expand it and identify which of its controls need to be replaced.

> **Tip**
>
> To more quickly identify controls, enter **`Replacement available`** in the search box.

7. Remove affected controls by selecting the check box and choosing **Remove from control set**.

8. Re-add the same controls. This action replaces the controls that you just removed with the latest control definition.

   a. Under **Add controls**, use the **Control type** dropdown list and select **Standard controls**.

   b. Find the replacement for the control that you just removed.

   > **Tip**
   >
   > In some cases, the replacement control name might not be exactly the same as the original. In this event, the replacement control name is likely to be very similar to the original. In rare cases, one control might be replaced by two controls (or the other way around).
   > If you can't find a replacement control, we recommend that you do a partial search. To do this, enter part of the original control name or a keyword that represents what you're looking for. You can also search by compliance type to further narrow the list of results.

   c. Select the check box next to a control and choose **Add to control set**.

   d. In the pop-up window that appears, choose **Add** to confirm.

9. Repeat steps 6-8 as needed until you have replaced all controls.
10. Choose **Next**.
11. On the **Review and save** page, choose **Save changes**.

I can’t make a copy of my custom framework

If the **Make a copy** button is unavailable on the framework details page, this means that you need to replace some of the controls in your custom framework.

For instructions on how to proceed, see On my custom framework details page, I’m prompted to recreate my custom framework.

My sent share request status displays as *Failed*

If you try to share a custom framework and the operation fails, we recommend that you check the following:

1. Make sure that Audit Manager is enabled in the recipient's AWS account and in the specified Region. For a list of supported AWS Audit Manager Regions, see AWS Audit Manager endpoints and quotas in the *Amazon Web Services General Reference*.
2. Make sure that you entered the correct AWS account ID when you specified the recipient account.
3. Make sure that you didn't specify an AWS Organizations management account as the recipient. You can share a custom framework with a delegated administrator, but if you try to share a custom framework with a management account, the operation fails.
4. If you use a customer managed key to encrypt your Audit Manager data, make sure that your KMS key is enabled. If your KMS key is disabled and you try to share a custom framework, the operation fails. For instructions on how to enable a disabled KMS key, see Enabling and disabling keys in the *AWS Key Management Service Developer Guide*.

My share request has a blue dot next to it. What does this mean?

A blue dot notification indicates that a share request needs your attention.

Blue dot notifications for senders

A blue notification dot appears next to sent share requests with a status of *Expiring*. Audit Manager displays the blue dot notification so that you can remind the recipient to take action on the share request before it expires.

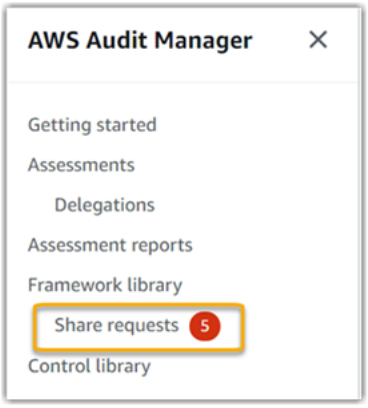
For the blue notification dot to disappear, the recipient must accept or decline the request. The blue dot also disappears if you revoke the share request.

You can use the following procedure to check for any expiring share requests, and send an optional reminder to the recipient to take action.

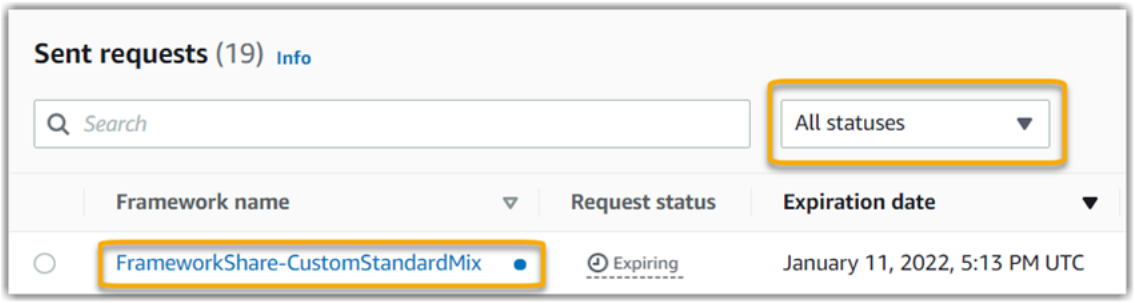
To view notifications for sent requests

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. If you have a share request notification, Audit Manager displays a red dot next to the navigation menu icon.

3. Expand the navigation pane and look next to **Share requests**. A notification badge indicates the number of share requests that need attention.



4. Choose **Share requests**, and then choose the **Sent requests** tab.
5. Look for the blue dot to identify share requests that expire within the next 30 days. Alternatively, you can also view expiring share requests by selecting **Expiring** from the **All statuses** filter dropdown.



6. (Optional) Remind the recipient that they need to take action on the share request before it expires. This step is optional, as Audit Manager sends a notification in the console to inform the recipient when a share request is active or expiring. However, you can also send your own reminder to the recipient using your preferred communication channel.

Blue dot notifications for recipients

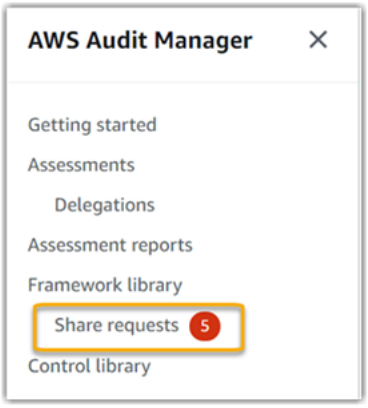
A blue notification dot appears next to received share requests with a status of *Active* or *Expiring*. Audit Manager displays the blue dot notification to remind you to take action on the share request before it expires. For the blue notification dot to disappear, you must accept or decline the request. The blue dot also disappears if the sender revokes the share request.

You can use the following procedure to check for active and expiring share requests.

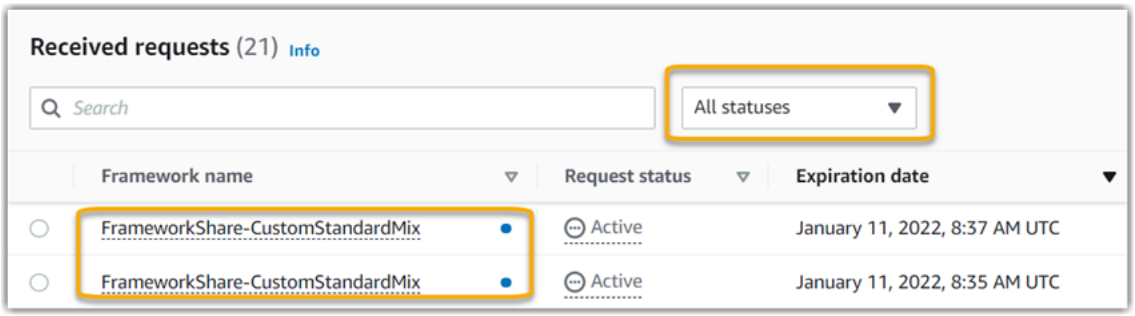
To view notifications for received requests

1. Open the AWS Audit Manager console at https://console.aws.amazon.com/auditmanager/home.
2. If you have a share request notification, Audit Manager displays a red dot next to the navigation menu icon.

3. Expand the navigation pane and look next to **Share requests**. A notification badge indicates the number of share requests that need your attention.



4. Choose **Share requests**. By default, this page opens on the **Received requests** tab.
5. Identify the share requests that need your action by looking for items with a blue dot.



6. (Optional) To view only requests that expire in the next 30 days, find the **All statuses** dropdown list and select **Expiring**.

My shared framework has controls that use custom AWS Config rules as a data source. Can the recipient collect evidence for these controls?

Yes, your recipient can collect evidence for these controls, but a few steps are needed to achieve this.

For Audit Manager to collect evidence using an AWS Config rule as a data source mapping, the following must be true. These criteria apply to both managed rules and custom rules.

- The rule must exist in the recipient's AWS environment.
- The rule must be enabled in the recipient's AWS environment.

Remember that the AWS Config rules in your account likely don't exist already in the recipient's AWS environment. Moreover, when the recipient accepts the share request, Audit Manager doesn't recreate any of your custom rules in their account. For the recipient to collect evidence using your custom rules as a data source mapping, they must create the same custom rules in their instance of AWS Config. After the recipient creates and then enables the rules in AWS Config, Audit Manager can collect evidence from that data source.

We recommend that you communicate with the recipient to let them know if any custom AWS Config rules should be created in their instance of AWS Config.

I updated a custom rule that's used in a shared framework. Do I need to take any action?

For rule updates within your AWS environment

When you update a custom rule within your AWS environment, no action is needed in Audit Manager. Audit Manager detects and handles rule updates in the way that's described in the following table. Audit Manager doesn't notify you when a rule update is detected.

Scenario	What Audit Manager does	What you need to do
A custom rule is **updated** in your instance of AWS Config.	Audit Manager continues to report findings for that rule using the updated rule definition.	No action is needed.
A custom rule is **deleted** in your instance of AWS Config.	Audit Manager stops reporting findings for the deleted rule.	No action is needed. If you want to, you can edit the custom controls that used the deleted rule as a data source mapping. You can then

Scenario	What Audit Manager does	What you need to do
		remove the deleted rule to clean up your control's data source settings. Otherwise, the deleted rule name remains as an unused data source mapping.

For rule updates outside your AWS environment

In the recipient's AWS environment, Audit Manager doesn't detect the rule update. This is because senders and recipients each work in separate AWS environments. The following table provides recommended actions for this scenario.

Your role	Scenario	Recommended action
Sender	• You shared a framework that uses custom rules as a data source mapping. • After you shared the framework, you updated or deleted one of those rules in AWS Config.	Contact the recipient to let them know about the update. That way, they can make the same update and stay in sync with the latest rule definition.
Recipie	• You accepted a shared framework that uses custom rules as a data source mapping. • After you recreated the custom rules in your instance of AWS Config, the sender updated or deleted one of those rules.	Make the corresponding rule update in your own instance of AWS Config.

Troubleshooting notification issues

You can use the information on this page to resolve common notification issues in Audit Manager.

Topics

I specified an Amazon SNS topic in Audit Manager, but I'm not receiving any notifications

If your Amazon SNS topic uses AWS KMS for server-side encryption (SSE), you might be missing the required permissions for your AWS KMS key policy. You might also fail to receive notifications if you didn't subscribe an endpoint to your topic.

If you aren't receiving notifications, make sure that you did the following:

- You attached the required permissions policy to your KMS key. For an example policy that you can use, see Example 2 (Permissions for the KMS key that's attached to the SNS topic).
- You subscribed an endpoint to the topic that the notifications are sent through. When you subscribe an email endpoint to a topic, you receive an email asking you to confirm your subscription. You must confirm your subscription to start receiving email notifications. For more information, see Getting Started in the Amazon SNS Developer Guide.

I specified a FIFO topic, but I'm not receiving notifications in the expected order

Audit Manager supports sending notifications to FIFO SNS topics. However, the order in which Audit Manager sends notifications to your FIFO topics isn't guaranteed.

Troubleshooting permission and access issues

You can use the information on this page to resolve common permission issues in Audit Manager.

Topics

I followed the Audit Manager setup procedure, but I don't have enough IAM privileges

The user, role, or group that you use to access Audit Manager must have the required permissions. Moreover, your identity-based policy shouldn't be too restrictive. Otherwise, the console won't function as intended. This guide provides an example policy that you can use to Allow the minimum permissions required to enable Audit Manager. Depending on your use case, you might need broader, less restrictive permissions. For example, we recommend that audit owners have administrator access. This is so that they can modify Audit Manager settings and manage resources such as assessments, frameworks, controls, and assessment reports. Other users, such as delegates, might only need management access or read-only access.

Make sure that you add the appropriate permissions for your user, role, or group. For audit owners, the recommended policy is AWSAuditManagerAdministratorAccess. For delegates, you can use the management access example policy that's provided on the IAM policy examples page. You can use these example policies as a starting point, and make changes as necessary to fit your requirements.

We recommend that you take time to customize your permissions to meet your specific requirements. If you need help with IAM permissions, contact your administrator or AWS Support.

I specified someone as an audit owner, but they still don’t have full access to the assessment. Why is this?

Specifying someone as an audit owner alone doesn't provide them with full access to an assessment. Audit owners must also have the necessary IAM permissions to access and manage Audit Manager resources. In other words, in addition to specifying a user as an audit owner, you must also attach the necessary IAM policies to that user. The idea behind this is that, by requiring both, Audit Manager ensures that you have full control over all of the specifics of each assessment.

> **Note**
>
> For audit owners, we recommend that you use the AWSAuditManagerAdministratorAccess policy. For more information, see Recommended policies for user personas in AWS Audit Manager.

I can't perform an action in Audit Manager

If you don't have the necessary permissions to use the AWS Audit Manager console or Audit Manager API operations, you will likely encounter an `AccessDeniedException` error.

To resolve this issue, you must contact your administrator for assistance. Your administrator is the person that provided you with your sign-in credentials.

I want to allow people outside of my AWS account to access my Audit Manager resources

You can create a role that users in other accounts or people outside of your organization can use to access your resources. You can specify who is trusted to assume the role. For services that support resource-based policies or access control lists (ACLs), you can use those policies to grant people access to your resources.

To learn more, consult the following:

- To learn whether Audit Manager supports these features, see How AWS Audit Manager works with IAM.
- To learn how to provide access to your resources across AWS accounts that you own, see Providing access to an IAM user in another AWS account that you own in the *IAM User Guide*.
- To learn how to provide access to your resources to third-party AWS accounts, see Providing access to AWS accounts owned by third parties in the *IAM User Guide*.
- To learn how to provide access through identity federation, see Providing access to externally authenticated users (identity federation) in the *IAM User Guide*.
- To learn the difference between using roles and resource-based policies for cross-account access, see Cross account resource access in IAM in the *IAM User Guide*.

I see an Access Denied error, despite having the required Audit Manager permissions

If your account is a part of an organization, it's possible that the `Access Denied` error is caused by a service control policy (SCP). SCPs are policies that are used to manage permissions for an organization. When an SCP is in place, it can deny specific permissions to all member accounts, including the delegated administrator account that you use in Audit Manager.

For example, if your organization has an SCP in place that denies permissions for AWS Control Catalog APIs, you can't view the resources that are provided by Control Catalog. This is true even if you otherwise have the required permissions for Audit Manager, such as the AWSAuditManagerAdministratorAccess policy. The SCP overrides the managed policy permissions by explicitly denying access to the Control Catalog APIs.

Here's an example of such an SCP. With this SCP in place, your delegated administrator account is denied access to the common controls, control objectives, and control domains that are needed to use the common controls feature in Audit Manager.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "controlcatalog:ListCommonControls",
                "controlcatalog:ListObjectives",
                "controlcatalog:ListDomains"
            ],
            "Resource": "*"
        }
    ]
}
```

To resolve this issue, we recommend that you take the following steps:

1. Confirm if an SCP is attached to your organization. For instructions, see Getting information about your organization's policies in the *AWS Organizations User Guide*.
2. Identify if the SCP is causing the `Access Denied` error.
3. Update the SCP to ensure that your delegated administrator account has the necessary access for Audit Manager. For instructions, see Updating an SCP in the *AWS Organizations User Guide*.

Additional resources

The following pages contain troubleshooting guidance for other issues that can be caused by missing permissions:

- I can’t see any controls or control sets in my assessment
- The custom rule option is unavailable when I’m configuring a control data source
- I get an *access denied* error when I try to generate a report
- I get an *access denied* error when I try to generate an assessment report using my delegated administrator account
- I can't enable evidence finder
- I can't disable evidence finder
- My search query fails
- I specified an Amazon SNS topic in Audit Manager, but I'm not receiving any notifications

Tagging AWS Audit Manager resources

A *tag* is a metadata label that you assign or that AWS assigns to an AWS resource. Each tag consists of a *key* and a *value*. For tags that you assign, you define the key and value. For example, you might define the key as `stage` and the value for one resource as `test`.

Tags help you do the following:

- Easily locate your Audit Manager resources. You can use tags as search criteria when browsing the framework library and the control library.
- Associate your resource with a compliance type. You can tag multiple resources with a compliance-specific tag to associate those resources with a specific framework.
- Identify and organize your AWS resources. Many AWS services support tagging, so you can assign the same tag to resources from different services to indicate that the resources are related.
- Track your AWS costs. You activate these tags on the AWS Billing and Cost Management dashboard. AWS uses the tags to categorize your costs and deliver a monthly cost allocation report to you. For more information, see Use cost allocation tags in the *AWS Billing and Cost Management User Guide*.

The following sections provide more information about tags for AWS Audit Manager.

Contents

Supported resources in Audit Manager

The following Audit Manager resources support tagging:

- Assessments
- Controls
- Frameworks

Tag restrictions

The following basic restrictions apply to tags on Audit Manager resources:

- Maximum number of tags that you can assign to a resource — 50
- Maximum key length — 128 Unicode characters
- Maximum value length — 256 Unicode characters
- Valid characters for key and value — a-z, A-Z, 0-9, space, and the following characters: _ . : / = + - and @
- Keys and values are case sensitive
- Don't use `aws:` as a prefix for keys; it's reserved for AWS use

Additional resources

You can set tags as properties when you create an assessment, framework, or control. You can add, edit, and delete tags through the Audit Manager console, the AWS Command Line Interface (AWS CLI), and the Audit Manager API. For more information, see the following links.

- For tagging assessments:
  - Creating an assessment in AWS Audit Manager and Editing an assessment in AWS Audit Manager in the *Assessments* section of this guide
  - Tags tab in the *Review an assessment* page of this guide
  - CreateAssessment and UpdateAssessment in the *AWS Audit Manager API Reference*
  - TagResource and UntagResource in the *AWS Audit Manager API Reference*
- For tagging frameworks:
  - Creating a custom framework in AWS Audit Manager and Editing a custom framework in AWS Audit Manager in the *Framework library* section of this guide
  - The Tags tab on the *View framework details* page of this guide
  - CreateAssessmentFramework and UpdateAssessmentFramework in the *AWS Audit Manager API Reference*
  - TagResource and UntagResource in the *AWS Audit Manager API Reference*
- For tagging controls:
  - Creating a custom control in AWS Audit Manager and Editing a custom control in AWS Audit Manager in the *Control library* section of this guide

- The Tags section on the *Reviewing a custom control* page of this guide
- The Tags section on the *Reviewing a standard control* page of this guide
- CreateControl and UpdateControl in the *AWS Audit Manager API Reference*
- TagResource and UntagResource in the *AWS Audit Manager API Reference*

Understanding quotas and restrictions for AWS Audit Manager

Your AWS account has default quotas, formerly referred to as *limits*, for each AWS service. Unless otherwise noted, each quota is Region-specific. You can request increases for some quotas, and other quotas can't be increased.

Most Audit Manager quotas, but not all, are listed under the AWS Audit Manager namespace in the Service Quotas console. To learn how to request a quota increase, see Managing your Audit Manager quotas.

Contents

Default Audit Manager quotas

The following AWS Audit Manager quotas are per AWS account per Region.

Resource	Quota
Assessments	Number of active assessments per account: 100
Assessment reports	Number of evidence items that you can add to an assessment report: • For same-Region reports (where the assessment and the assessment report destination S3 bucket are in the same AWS Region): 22,000 • For cross-Region reports (where the assessment and the assessment report destination S3 bucket are in different AWS Regions): 3,500 • For reports where the related assessment uses a customer managed AWS KMS key: 3,500

Resource	Quota
Controls	Number of custom controls per account: 500
Evidence	Maximum size of a single manual evidence file: 100 MB Number of daily manual evidence uploads per control: 100 **Tip** If you need to upload a large amount of manual evidence to a single control, we recommend that you upload your evidence in batches across several days.
Frameworks	Number of custom frameworks per account: 100 **Note** Framework quotas apply to all shared custom framework s in your framework library, regardless of who created the framework.
Shared custom framework recipients	Number of active recipient accounts: 100
API access	Number of transactions per second (TPS) across all APIs: 20 TPS

Managing your Audit Manager quotas

AWS Audit Manager is integrated with Service Quotas, an AWS service that enables you to view and manage your quotas from a central location. Service Quotas makes it easy to look up the value of your Audit Manager quotas.

To view Audit Manager service quotas using the console

1. Open the Service Quotas console at https://console.aws.amazon.com/servicequotas/.
2. In the navigation pane, choose **AWS services**.

3. From the **AWS services** list, search for and select **AWS Audit Manager**.
4. In the **Service quotas** list, you can see the service quota name, applied quota value (if it's available), AWS default quota value, and whether the quota is adjustable.
5. To view additional information about a service quota, such as the description, choose the quota name.
6. (Optional) To request a quota increase, select the quota that you want to increase, select **Request quota increase**, enter or select the required information, and select **Request**.

Additional resources

For more information about how to manage your quotas, see Requesting a quota increase in the *Service Quotas User Guide*.

For more information about Service Quotas, see What Is Service Quotas? in the *Service Quotas User Guide*.

Code examples for Audit Manager using AWS SDKs

The following code examples show how to use Audit Manager with an AWS software development kit (SDK).

Scenarios are code examples that show you how to accomplish specific tasks by calling multiple functions within a service or combined with other AWS services.

For a complete list of AWS SDK developer guides and code examples, see Using AWS Audit Manager with an AWS SDK. This topic also includes information about getting started and details about previous SDK versions.

Code examples

- Scenarios for Audit Manager using AWS SDKs
  - Create an Audit Manager custom framework from an AWS Config conformance pack using an AWS SDK
  - Create an Audit Manager custom framework that contains Security Hub controls using an AWS SDK
  - Create an Audit Manager assessment report that contains one day of evidence using an AWS SDK

Scenarios for Audit Manager using AWS SDKs

The following code examples show you how to implement common scenarios in Audit Manager with AWS SDKs. These scenarios show you how to accomplish specific tasks by calling multiple functions within Audit Manager or combined with other AWS services. Each scenario includes a link to the complete source code, where you can find instructions on how to set up and run the code.

Scenarios target an intermediate level of experience to help you understand service actions in context.

Examples

- Create an Audit Manager custom framework from an AWS Config conformance pack using an AWS SDK
- Create an Audit Manager custom framework that contains Security Hub controls using an AWS SDK

- Create an Audit Manager assessment report that contains one day of evidence using an AWS SDK

Create an Audit Manager custom framework from an AWS Config conformance pack using an AWS SDK

The following code example shows how to:

- Get a list of AWS Config conformance packs.
- Create an Audit Manager custom control for each managed rule in a conformance pack.
- Create an Audit Manager custom framework that contains the controls.

Python

SDK for Python (Boto3)

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
import logging
import boto3
from botocore.exceptions import ClientError

logger = logging.getLogger(__name__)


class ConformancePack:
    def __init__(self, config_client, auditmanager_client):
        self.config_client = config_client
        self.auditmanager_client = auditmanager_client

    def get_conformance_pack(self):
        """
        Return a selected conformance pack from the list of conformance packs.

        :return: selected conformance pack
        """
```

```
        try:
            conformance_packs = self.config_client.describe_conformance_packs()
            print(
                "Number of conformance packs fetched: ",
                len(conformance_packs.get("ConformancePackDetails")),
            )
            print("Fetched the following conformance packs: ")
            all_cpack_names = {
                cp["ConformancePackName"]
                for cp in conformance_packs.get("ConformancePackDetails")
            }
            for pack in all_cpack_names:
                print(f"\t{pack}")
            cpack_name = input(
                "Provide ConformancePackName that you want to create a custom "
                "framework for: "
            )
            if cpack_name not in all_cpack_names:
                print(f"{cpack_name} is not in the list of conformance packs!")
                print(
                    "Provide a conformance pack name from the available list of "
                    "conformance packs."
                )
                raise Exception("Invalid conformance pack")
            print("-" * 88)
        except ClientError:
            logger.exception("Couldn't select conformance pack.")
            raise
        else:
            return cpack_name

    def create_custom_controls(self, cpack_name):
        """
        Create custom controls for all managed AWS Config rules in a conformance
pack.

        :param cpack_name: The name of the conformance pack to create controls
for.
        :return: The list of custom control IDs.
        """
        try:
            rules_in_pack =
self.config_client.describe_conformance_pack_compliance(
                ConformancePackName=cpack_name
```

```
            )
            print(
                "Number of rules in the conformance pack: ",
                len(rules_in_pack.get("ConformancePackRuleComplianceList")),
            )
            for rule in rules_in_pack.get("ConformancePackRuleComplianceList"):
                print(f"\t{rule.get('ConfigRuleName')}")
            print("-" * 88)
            print(
                "Creating a custom control for each rule and a custom framework "
                "consisting of these rules in Audit Manager."
            )
            am_controls = []
            for rule in rules_in_pack.get("ConformancePackRuleComplianceList"):
                config_rule = self.config_client.describe_config_rules(
                    ConfigRuleNames=[rule.get("ConfigRuleName")]
                )
                source_id = (
                    config_rule.get("ConfigRules")[0]
                    .get("Source", {})
                    .get("SourceIdentifier")
                )
                custom_control = self.auditmanager_client.create_control(
                    name="Config-" + rule.get("ConfigRuleName"),
                    controlMappingSources=[
                        {
                            "sourceName": "ConfigRule",
                            "sourceSetUpOption": "System_Controls_Mapping",
                            "sourceType": "AWS_Config",
                            "sourceKeyword": {
                                "keywordInputType": "SELECT_FROM_LIST",
                                "keywordValue": source_id,
                            },
                        }
                    ],
                ).get("control", {})
                am_controls.append({"id": custom_control.get("id")})
            print("Successfully created a control for each config rule.")
            print("-" * 88)
        except ClientError:
            logger.exception("Failed to create custom controls.")
            raise
        else:
            return am_controls
```

```
    def create_custom_framework(self, cpack_name, am_control_ids):
        """
        Create a custom Audit Manager framework from a selected AWS Config
 conformance
        pack.

        :param cpack_name: The name of the conformance pack to create a framework
 from.
        :param am_control_ids: The IDs of the custom controls created from the
                               conformance pack.
        """
        try:
            print("Creating custom framework...")
            custom_framework =
 self.auditmanager_client.create_assessment_framework(
                name="Config-Conformance-pack-" + cpack_name,
                controlSets=[{"name": cpack_name, "controls": am_control_ids}],
            )
            print(
                f"Successfully created the custom framework: ",
                f"{custom_framework.get('framework').get('name')}: ",
                f"{custom_framework.get('framework').get('id')}",
            )
            print("-" * 88)
        except ClientError:
            logger.exception("Failed to create custom framework.")
            raise


def run_demo():
    print("-" * 88)
    print("Welcome to the AWS Audit Manager custom framework demo!")
    print("-" * 88)
    print(
        "You can use this sample to select a conformance pack from AWS Config and
 "
        "use AWS Audit Manager to create a custom control for all the managed "
        "rules under the conformance pack. A custom framework is also created "
        "with these controls."
    )
    print("-" * 88)
    conf_pack = ConformancePack(boto3.client("config"),
 boto3.client("auditmanager"))
```

```
    cpack_name = conf_pack.get_conformance_pack()
    am_controls = conf_pack.create_custom_controls(cpack_name)
    conf_pack.create_custom_framework(cpack_name, am_controls)


if __name__ == "__main__":
    run_demo()
```

- For API details, see the following topics in *AWS SDK for Python (Boto3) API Reference*.
  - CreateAssessmentFramework
  - CreateControl

For a complete list of AWS SDK developer guides and code examples, see Using AWS Audit Manager with an AWS SDK. This topic also includes information about getting started and details about previous SDK versions.

Create an Audit Manager custom framework that contains Security Hub controls using an AWS SDK

The following code example shows how to:

- Get a list of all standard controls that have Security Hub as their data source.
- Create an Audit Manager custom framework that contains the controls.

Python

SDK for Python (Boto3)

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
import logging
import boto3
from botocore.exceptions import ClientError
```

```
logger = logging.getLogger(__name__)


class SecurityHub:
    def __init__(self, auditmanager_client):
        self.auditmanager_client = auditmanager_client

    def get_sechub_controls(self):
        """
        Gets the list of controls that use Security Hub as their data source.

        :return: The list of Security Hub controls.
        """
        print("-" * 88)
        next_token = None
        page = 1
        sechub_control_list = []
        while True:
            print("Page [" + str(page) + "]")
            if next_token is None:
                control_list = self.auditmanager_client.list_controls(
                    controlType="Standard", maxResults=100
                )
            else:
                control_list = self.auditmanager_client.list_controls(
                    controlType="Standard", nextToken=next_token, maxResults=100
                )
            print("Total controls found:",
 len(control_list.get("controlMetadataList")))
            for control in control_list.get("controlMetadataList"):
                control_details = self.auditmanager_client.get_control(
                    controlId=control.get("id")
                ).get("control", {})
                if "AWS Security Hub" in control_details.get("controlSources"):
                    sechub_control_list.append({"id": control_details.get("id")})
            next_token = control_list.get("nextToken")
            if not next_token:
                break
            page += 1
        print("Number of Security Hub controls found: ",
 len(sechub_control_list))
        return sechub_control_list
```

```
    def create_custom_framework(self, am_controls):
        """
        Create a custom framework with a list of controls.

        :param am_controls: The list of controls to include in the framework.
        """
        try:
            print("Creating custom framework...")
            custom_framework =
 self.auditmanager_client.create_assessment_framework(
                name="All Security Hub Controls Framework",
                controlSets=[{"name": "Security-Hub", "controls": am_controls}],
            )
            print(
                f"Successfully created the custom framework: "
                f"{custom_framework.get('framework').get('name')}: "
                f"{custom_framework.get('framework').get('id')}"
            )
            print("-" * 88)
        except ClientError:
            logger.exception("Failed to create custom framework.")
            raise


def run_demo():
    print("-" * 88)
    print("Welcome to the AWS Audit Manager Security Hub demo!")
    print("-" * 88)
    print(" This script creates a custom framework with all Security Hub
 controls.")
    print("-" * 88)
    sechub = SecurityHub(boto3.client("auditmanager"))
    am_controls = sechub.get_sechub_controls()
    sechub.create_custom_framework(am_controls)


if __name__ == "__main__":
    run_demo()
```

- For API details, see the following topics in *AWS SDK for Python (Boto3) API Reference*.
  - CreateAssessmentFramework
  - GetControl

- ListControls

For a complete list of AWS SDK developer guides and code examples, see Using AWS Audit Manager with an AWS SDK. This topic also includes information about getting started and details about previous SDK versions.

Create an Audit Manager assessment report that contains one day of evidence using an AWS SDK

The following code example shows how to create an Audit Manager assessment report that contains one day of evidence.

Python

SDK for Python (Boto3)

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
import dateutil.parser
import logging
import time
import urllib.request
import uuid
import boto3
from botocore.exceptions import ClientError


logger = logging.getLogger(__name__)


class AuditReport:
    def __init__(self, auditmanager_client):
        self.auditmanager_client = auditmanager_client

    def get_input(self):
        print("-" * 40)
```

```
        try:
            assessment_id = input("Provide assessment id [uuid]: ").lower()
            try:
                assessment_uuid = uuid.UUID(assessment_id)
            except ValueError:
                logger.error("Assessment Id is not a valid UUID: %s",
assessment_id)
                raise
            evidence_folder = input("Provide evidence date [yyyy-mm-dd]: ")
            try:
                evidence_date = dateutil.parser.parse(evidence_folder).date()
            except ValueError:
                logger.error("Invalid date : %s", evidence_folder)
                raise
            try:
                self.auditmanager_client.get_assessment(
                    assessmentId=str(assessment_uuid)
                )
            except ClientError:
                logger.exception("Couldn't get assessment %s.", assessment_uuid)
                raise
        except (ValueError, ClientError):
            return None, None
        else:
            return assessment_uuid, evidence_date

    def clear_staging(self, assessment_uuid, evidence_date):
        """
        Find all the evidence in the report and clear it.
        """
        next_token = None
        page = 1
        interested_folder_id_list = []
        while True:
            print(f"Page [{page}]")
            if next_token is None:
                folder_list = (
                    self.auditmanager_client.get_evidence_folders_by_assessment(
                        assessmentId=str(assessment_uuid), maxResults=1000
                    )
                )
            else:
                folder_list = (
                    self.auditmanager_client.get_evidence_folders_by_assessment(
```

```
                        assessmentId=str(assessment_uuid),
                        nextToken=next_token,
                        maxResults=1000,
                    )
                )
            folders = folder_list.get("evidenceFolders")
            print(f"Got {len(folders)} folders.")
            for folder in folders:
                folder_id = folder.get("id")
                if folder.get("name") == str(evidence_date):
                    interested_folder_id_list.append(folder_id)
                if folder.get("assessmentReportSelectionCount") == folder.get(
                    "totalEvidence"
                ):
                    print(
                        f"Removing folder from report selection :
{folder.get('name')} "
                        f"{folder_id} {folder.get('controlId')}"
                    )

self.auditmanager_client.disassociate_assessment_report_evidence_folder(
                        assessmentId=str(assessment_uuid),
evidenceFolderId=folder_id
                    )
                elif folder.get("assessmentReportSelectionCount") > 0:
                    # Get all evidence in the folder and
                    # add selected evidence in the selected_evidence_list.
                    evidence_list = (
                        self.auditmanager_client.get_evidence_by_evidence_folder(
                            assessmentId=str(assessment_uuid),
                            controlSetId=folder_id,
                            evidenceFolderId=folder_id,
                            maxResults=1000,
                        )
                    )
                    selected_evidence_list = []
                    for evidence in evidence_list.get("evidence"):
                        if evidence.get("assessmentReportSelection") == "Yes":
                            selected_evidence_list.append(evidence.get("id"))
                    print(
                        f"Removing evidence report selection :
{folder.get('name')} "
                        f"{len(selected_evidence_list)}"
                    )
```

```
self.auditmanager_client.batch_disassociate_assessment_report_evidence(
                        assessmentId=str(assessment_uuid),
                        evidenceFolderId=folder_id,
                        evidenceIds=selected_evidence_list,
                    )
            next_token = folder_list.get("nextToken")
            if not next_token:
                break
            page += 1
        return interested_folder_id_list

    def add_folder_to_staging(self, assessment_uuid, folder_id_list):
        print(f"Adding folders to report : {folder_id_list}")
        for folder in folder_id_list:
            self.auditmanager_client.associate_assessment_report_evidence_folder(
                assessmentId=str(assessment_uuid), evidenceFolderId=folder
            )

    def get_report(self, assessment_uuid):
        report = self.auditmanager_client.create_assessment_report(
            name="ReportViaScript",
            description="testing",
            assessmentId=str(assessment_uuid),
        )
        if self._is_report_generated(report.get("assessmentReport").get("id")):
            report_url = self.auditmanager_client.get_assessment_report_url(
                assessmentReportId=report.get("assessmentReport").get("id"),
                assessmentId=str(assessment_uuid),
            )
            print(report_url.get("preSignedUrl"))
            urllib.request.urlretrieve(
                report_url.get("preSignedUrl").get("link"),
                report_url.get("preSignedUrl").get("hyperlinkName"),
            )
            print(
                f"Report saved as
{report_url.get('preSignedUrl').get('hyperlinkName')}."
            )
        else:
            print("Report generation did not finish in 15 minutes.")
            print(
                "Failed to download report. Go to the console and manually
download "
```

```
                "the report."
            )

    def _is_report_generated(self, assessment_report_id):
        max_wait_time = 0
        while max_wait_time < 900:
            print(f"Checking status of the report {assessment_report_id}")
            report_list =
 self.auditmanager_client.list_assessment_reports(maxResults=1)
            if (
                report_list.get("assessmentReports")[0].get("id")
                == assessment_report_id
                and report_list.get("assessmentReports")[0].get("status") ==
 "COMPLETE"
            ):
                return True
            print("Sleeping for 5 seconds...")
            time.sleep(5)
            max_wait_time += 5


def run_demo():
    print("-" * 88)
    print("Welcome to the AWS Audit Manager samples demo!")
    print("-" * 88)
    print(
        "This script creates an assessment report for an assessment with all the
 "
        "evidence collected on the provided date."
    )
    print("-" * 88)

    report = AuditReport(boto3.client("auditmanager"))
    assessment_uuid, evidence_date = report.get_input()
    if assessment_uuid is not None and evidence_date is not None:
        folder_id_list = report.clear_staging(assessment_uuid, evidence_date)
        report.add_folder_to_staging(assessment_uuid, folder_id_list)
        report.get_report(assessment_uuid)


if __name__ == "__main__":
    run_demo()
```

- For API details, see the following topics in *AWS SDK for Python (Boto3) API Reference*.
  - AssociateAssessmentReportEvidenceFolder
  - BatchDisassociateAssessmentReportEvidence
  - CreateAssessmentReport
  - DisassociateAssessmentReportEvidenceFolder
  - GetAssessment
  - GetAssessmentReportUrl
  - GetEvidenceByEvidenceFolder
  - GetEvidenceFoldersByAssessment
  - ListAssessmentReports

For a complete list of AWS SDK developer guides and code examples, see Using AWS Audit Manager with an AWS SDK. This topic also includes information about getting started and details about previous SDK versions.

Understanding security and data protection in AWS Audit Manager

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 Audit Manager, 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 Audit Manager. The following topics show you how to configure Audit Manager to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your Audit Manager resources.

Topics

Data protection in AWS Audit Manager

The AWS shared responsibility model applies to data protection in AWS Audit Manager. 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. You are also responsible for 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 users with AWS IAM Identity Center or 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 require TLS 1.2 and recommend TLS 1.3.
- Set up API and user activity logging with AWS CloudTrail. For information about using CloudTrail trails to capture AWS activities, see Working with CloudTrail trails in the *AWS CloudTrail User Guide*.
- 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 sensitive data that is stored in Amazon S3.
- If you require FIPS 140-3 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) 140-3.

We strongly recommend that you never put confidential or sensitive information, such as your customers' email addresses, into tags or free-form text fields such as a **Name** field. This includes when you work with Audit Manager or other AWS services using the console, API, AWS CLI, or AWS SDKs. Any data that you enter into tags or free-form text fields used for names may be used for billing or diagnostic logs. If you provide a URL to an external server, we strongly recommend that you do not include credentials information in the URL to validate your request to that server.

In addition to the recommendation above, we recommend specifically that Audit Manager customers don't include sensitive identifying information in free-form fields when creating assessments, custom controls, custom frameworks, and delegation comments.

Deletion of Audit Manager data

There are several ways that Audit Manager data can be deleted.

Data deletion when disabling Audit Manager

When you disable Audit Manager, you can decide if you want to delete all of your Audit Manager data. If you choose to delete your data, it's deleted within 7 days of disabling Audit Manager. After your data is deleted, you can't recover it.

Automatic data deletion

Some Audit Manager data is deleted automatically after a specific period of time. Audit Manager retains customer data as follows.

Data type	Data retention period	Notes
Evidence	Data is retained for 2 years from the time of creation	Includes automated evidence and manual evidence
Customer-created resources	Data is retained indefinitely	Includes assessments, assessment reports, custom controls, and custom frameworks

Manual data deletion

You can delete individual Audit Manager resources at any time. For instructions, see the following:

- Deleting an assessment in AWS Audit Manager
  - See also: DeleteAssessment in the *AWS Audit Manager API Reference*
- Deleting a custom framework in AWS Audit Manager
  - See also: DeleteAssessmentFramework in the *AWS Audit Manager API Reference*

- Deleting share requests in AWS Audit Manager
  - See also: DeleteAssessmentFrameworkShare in the *AWS Audit Manager API Reference*
- Deleting an assessment report
  - See also: DeleteAssessmentReport in the *AWS Audit Manager API Reference*
- Deleting a custom control in AWS Audit Manager
  - See also: DeleteControl in the *AWS Audit Manager API Reference*

To delete other resource data that you might have created when using Audit Manager, see the following:

- Delete an event data store in the *AWS CloudTrail User Guide*
- Deleting a bucket in the *Amazon Simple Storage Service (Amazon S3) User Guide*

Encryption at rest

To encrypt data at rest, Audit Manager uses server-side encryption with AWS managed keys for all its data stores and logs.

Your data is encrypted under a customer managed key or an AWS owned key, depending on your selected settings. If you don't provide a customer managed key, Audit Manager uses an AWS owned key to encrypt your content. All service metadata in DynamoDB and Amazon S3 in Audit Manager is encrypted using an AWS owned key.

Audit Manager encrypts data as follows:

- Service metadata stored in Amazon S3 is encrypted under an AWS owned key using SSE-KMS.
- Service metadata stored in DynamoDB is server side encrypted using KMS and an AWS owned key.
- Your content stored in DynamoDB is client-side encrypted using either a customer managed key or an AWS owned key. The KMS key is based on your chosen settings.
- Your content stored in Amazon S3 in Audit Manager is encrypted using SSE-KMS. The KMS key is based on your selection, and could be either a customer managed key or an AWS owned key.
- The assessment reports published to your S3 bucket are encrypted as follows:
  - If you provided a customer managed key, your data is encrypted using SSE-KMS.
  - If you used the AWS owned key, your data is encrypted using SSE-S3.

Encryption in transit

Audit Manager provides secure and private endpoints for encrypting data in transit. The secure and private endpoints allow AWS to protect the integrity of API requests to Audit Manager.

Inter-service transit

By default, all inter-service communications are protected by using Transport Layer Security (TLS) encryption.

Key management

Audit Manager supports both AWS owned keys and customer managed keys for encrypting all Audit Manager resources (assessments, controls, frameworks, evidence, and assessment reports saved to S3 buckets in your accounts).

We recommend that you use a customer managed key. By doing so, you can view and manage the encryption keys that protect your data, including viewing logs of their use in AWS CloudTrail. When you choose a customer managed key, Audit Manager creates a grant on the KMS key so that it can be used to encrypt your content.

> **Warning**
>
> After you delete or disable a KMS key that is used to encrypt Audit Manager resources, you can no longer decrypt the resource that was encrypted under that KMS key, which means that data becomes unrecoverable.
> Deleting a KMS key in AWS Key Management Service (AWS KMS) is destructive and potentially dangerous. For more information about deleting KMS keys, see Deleting AWS KMS keys in the *AWS Key Management Service User Guide*.

You can specify your encryption settings when you enable Audit Manager using the AWS Management Console, the Audit Manager API, or the AWS Command Line Interface (AWS CLI). For instructions, see Enabling AWS Audit Manager.

You can review and change your encryption settings at any time. For instructions, see Configuring your data encryption settings.

For more information about how to set up customer managed keys, see Creating keys in the *AWS Key Management Service User Guide*.

Identity and access management for AWS Audit Manager

AWS Identity and Access Management (IAM) is an AWS service that helps an administrator securely control access to AWS resources. IAM administrators control who can be *authenticated* (signed in) and *authorized* (have permissions) to use Audit Manager resources. IAM is an AWS service that you can use with no additional charge.

Topics

Audience

How you use AWS Identity and Access Management (IAM) differs, depending on the work that you do in Audit Manager.

Service user – If you use the Audit Manager service to do your job, then your administrator provides you with the credentials and permissions that you need. As you use more Audit Manager features to do your work, you might need additional permissions. Understanding how access is managed can help you request the right permissions from your administrator. If you cannot access a feature in Audit Manager, see Troubleshooting AWS Audit Manager identity and access.

Service administrator – If you're in charge of Audit Manager resources at your company, you probably have full access to Audit Manager. It's your job to determine which Audit Manager features and resources your service users should access. You must then submit requests to your IAM administrator to change the permissions of your service users. Review the information on this page

to understand the basic concepts of IAM. To learn more about how your company can use IAM with Audit Manager, see How AWS Audit Manager works with IAM.

IAM administrator – If you're an IAM administrator, you might want to learn details about how you can write policies to manage access to Audit Manager. To view example Audit Manager identity-based policies that you can use in IAM, see Identity-based policy examples for AWS Audit Manager.

Authenticating with identities

Authentication is how you sign in to AWS using your identity credentials. You must be *authenticated* (signed in to AWS) as the AWS account root user, as an IAM user, or by assuming an IAM role.

You can sign in to AWS as a federated identity by using credentials provided through an identity source. AWS IAM Identity Center (IAM Identity Center) users, your company's single sign-on authentication, and your Google or Facebook credentials are examples of federated identities. When you sign in as a federated identity, your administrator previously set up identity federation using IAM roles. When you access AWS by using federation, you are indirectly assuming a role.

Depending on the type of user you are, you can sign in to the AWS Management Console or the AWS access portal. For more information about signing in to AWS, see How to sign in to your AWS account in the *AWS Sign-In User Guide*.

If you access AWS programmatically, AWS provides a software development kit (SDK) and a command line interface (CLI) to cryptographically sign your requests by using your credentials. If you don't use AWS tools, you must sign requests yourself. For more information about using the recommended method to sign requests yourself, see AWS Signature Version 4 for API requests in the *IAM User Guide*.

Regardless of the authentication method that you use, you might be required to provide additional security information. For example, AWS recommends that you use multi-factor authentication (MFA) to increase the security of your account. To learn more, see Multi-factor authentication in the *AWS IAM Identity Center User Guide* and AWS Multi-factor authentication in IAM in the *IAM User Guide*.

AWS account root user

When you create an AWS account, you begin with one sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account *root user* and is accessed by signing in with the email address and password that you used to create the account.

We strongly recommend that you don't use the root user for your everyday tasks. Safeguard your root user credentials and use them to perform the tasks that only the root user can perform. For the complete list of tasks that require you to sign in as the root user, see Tasks that require root user credentials in the *IAM User Guide*.

Federated identity

As a best practice, require human users, including users that require administrator access, to use federation with an identity provider to access AWS services by using temporary credentials.

A *federated identity* is a user from your enterprise user directory, a web identity provider, the AWS Directory Service, the Identity Center directory, or any user that accesses AWS services by using credentials provided through an identity source. When federated identities access AWS accounts, they assume roles, and the roles provide temporary credentials.

For centralized access management, we recommend that you use AWS IAM Identity Center. You can create users and groups in IAM Identity Center, or you can connect and synchronize to a set of users and groups in your own identity source for use across all your AWS accounts and applications. For information about IAM Identity Center, see What is IAM Identity Center? in the *AWS IAM Identity Center User Guide*.

IAM users and groups

An *IAM user* is an identity within your AWS account that has specific permissions for a single person or application. Where possible, we recommend relying on temporary credentials instead of creating IAM users who have long-term credentials such as passwords and access keys. However, if you have specific use cases that require long-term credentials with IAM users, we recommend that you rotate access keys. For more information, see Rotate access keys regularly for use cases that require long-term credentials in the *IAM User Guide*.

An *IAM group* is an identity that specifies a collection of IAM users. You can't sign in as a group. You can use groups to specify permissions for multiple users at a time. Groups make permissions easier to manage for large sets of users. For example, you could have a group named *IAMAdmins* and give that group permissions to administer IAM resources.

Users are different from roles. A user is uniquely associated with one person or application, but a role is intended to be assumable by anyone who needs it. Users have permanent long-term credentials, but roles provide temporary credentials. To learn more, see Use cases for IAM users in the *IAM User Guide*.

IAM roles

An *IAM role* is an identity within your AWS account that has specific permissions. It is similar to an IAM user, but is not associated with a specific person. To temporarily assume an IAM role in the AWS Management Console, you can switch from a user to an IAM role (console). You can assume a role by calling an AWS CLI or AWS API operation or by using a custom URL. For more information about methods for using roles, see Methods to assume a role in the *IAM User Guide*.

IAM roles with temporary credentials are useful in the following situations:

- **Federated user access** – To assign permissions to a federated identity, you create a role and define permissions for the role. When a federated identity authenticates, the identity is associated with the role and is granted the permissions that are defined by the role. For information about roles for federation, see Create a role for a third-party identity provider (federation) in the *IAM User Guide*. If you use IAM Identity Center, you configure a permission set. To control what your identities can access after they authenticate, IAM Identity Center correlates the permission set to a role in IAM. For information about permissions sets, see Permission sets in the *AWS IAM Identity Center User Guide*.
- **Temporary IAM user permissions** – An IAM user or role can assume an IAM role to temporarily take on different permissions for a specific task.
- **Cross-account access** – You can use an IAM role to allow someone (a trusted principal) in a different account to access resources in your account. Roles are the primary way to grant cross-account access. However, with some AWS services, you can attach a policy directly to a resource (instead of using a role as a proxy). To learn the difference between roles and resource-based policies for cross-account access, see Cross account resource access in IAM in the *IAM User Guide*.
- **Cross-service access** – Some AWS services use features in other AWS services. For example, when you make a call in a service, it's common for that service to run applications in Amazon EC2 or store objects in Amazon S3. A service might do this using the calling principal's permissions, using a service role, or using a service-linked role.
  - **Forward access sessions (FAS)** – When you use an IAM user or role to perform actions in AWS, you are considered a principal. When you use some services, you might perform an action that then initiates another action in a different service. FAS uses the permissions of the principal calling an AWS service, combined with the requesting AWS service to make requests to downstream services. FAS requests are only made when a service receives a request that requires interactions with other AWS services or resources to complete. In this case, you must have permissions to perform both actions. For policy details when making FAS requests, see Forward access sessions.

- **Service role** – A service role is an IAM role that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see Create a role to delegate permissions to an AWS service in the *IAM User Guide*.
- **Service-linked role** – A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your AWS account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.

- **Applications running on Amazon EC2** – You can use an IAM role to manage temporary credentials for applications that are running on an EC2 instance and making AWS CLI or AWS API requests. This is preferable to storing access keys within the EC2 instance. To assign an AWS role to an EC2 instance and make it available to all of its applications, you create an instance profile that is attached to the instance. An instance profile contains the role and enables programs that are running on the EC2 instance to get temporary credentials. For more information, see Use an IAM role to grant permissions to applications running on Amazon EC2 instances in the *IAM User Guide*.

Managing access using policies

You control access in AWS by creating policies and attaching them to AWS identities or resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. AWS evaluates these policies when a principal (user, root user, or role session) makes a request. Permissions in the policies determine whether the request is allowed or denied. Most policies are stored in AWS as JSON documents. For more information about the structure and contents of JSON policy documents, see Overview of JSON policies in the *IAM User Guide*.

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

By default, users and roles have no permissions. To grant users permission to perform actions on the resources that they need, an IAM administrator can create IAM policies. The administrator can then add the IAM policies to roles, and users can assume the roles.

IAM policies define permissions for an action regardless of the method that you use to perform the operation. For example, suppose that you have a policy that allows the `iam:GetRole` action. A user with that policy can get role information from the AWS Management Console, the AWS CLI, or the AWS API.

Identity-based policies

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, group of users, or role. These policies control what actions users and roles can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see Define custom IAM permissions with customer managed policies in the *IAM User Guide*.

Identity-based policies can be further categorized as *inline policies* or *managed policies*. Inline policies are embedded directly into a single user, group, or role. Managed policies are standalone policies that you can attach to multiple users, groups, and roles in your AWS account. Managed policies include AWS managed policies and customer managed policies. To learn how to choose between a managed policy or an inline policy, see Choose between managed policies and inline policies in the *IAM User Guide*.

Resource-based policies

Resource-based policies are JSON policy documents that you attach to a resource. Examples of resource-based policies are IAM *role trust policies* and Amazon S3 *bucket policies*. In services that support resource-based policies, service administrators can use them to control access to a specific resource. For the resource where the policy is attached, the policy defines what actions a specified principal can perform on that resource and under what conditions. You must specify a principal in a resource-based policy. Principals can include accounts, users, roles, federated users, or AWS services.

Resource-based policies are inline policies that are located in that service. You can't use AWS managed policies from IAM in a resource-based policy.

Access control lists (ACLs)

Access control lists (ACLs) control which principals (account members, users, or roles) have permissions to access a resource. ACLs are similar to resource-based policies, although they do not use the JSON policy document format.

Amazon S3, AWS WAF, and Amazon VPC are examples of services that support ACLs. To learn more about ACLs, see Access control list (ACL) overview in the *Amazon Simple Storage Service Developer Guide*.

Other policy types

AWS supports additional, less-common policy types. These policy types can set the maximum permissions granted to you by the more common policy types.

- **Permissions boundaries** – A permissions boundary is an advanced feature in which you set the maximum permissions that an identity-based policy can grant to an IAM entity (IAM user or role). You can set a permissions boundary for an entity. The resulting permissions are the intersection of an entity's identity-based policies and its permissions boundaries. Resource-based policies that specify the user or role in the `Principal` field are not limited by the permissions boundary. An explicit deny in any of these policies overrides the allow. For more information about permissions boundaries, see Permissions boundaries for IAM entities in the *IAM User Guide*.
- **Service control policies (SCPs)** – SCPs are JSON policies that specify the maximum permissions for an organization or organizational unit (OU) in AWS Organizations. AWS Organizations is a service for grouping and centrally managing multiple AWS accounts that your business owns. If you enable all features in an organization, then you can apply service control policies (SCPs) to any or all of your accounts. The SCP limits permissions for entities in member accounts, including each AWS account root user. For more information about Organizations and SCPs, see Service control policies in the *AWS Organizations User Guide*.
- **Resource control policies (RCPs)** – RCPs are JSON policies that you can use to set the maximum available permissions for resources in your accounts without updating the IAM policies attached to each resource that you own. The RCP limits permissions for resources in member accounts and can impact the effective permissions for identities, including the AWS account root user, regardless of whether they belong to your organization. For more information about Organizations and RCPs, including a list of AWS services that support RCPs, see Resource control policies (RCPs) in the *AWS Organizations User Guide*.
- **Session policies** – Session policies are advanced policies that you pass as a parameter when you programmatically create a temporary session for a role or federated user. The resulting session's permissions are the intersection of the user or role's identity-based policies and the session policies. Permissions can also come from a resource-based policy. An explicit deny in any of these policies overrides the allow. For more information, see Session policies in the *IAM User Guide*.

Multiple policy types

When multiple types of policies apply to a request, the resulting permissions are more complicated to understand. To learn how AWS determines whether to allow a request when multiple policy types are involved, see Policy evaluation logic in the *IAM User Guide*.

How AWS Audit Manager works with IAM

Before you use IAM to manage access to Audit Manager, learn what IAM features are available to use with Audit Manager.

IAM features you can use with AWS Audit Manager

IAM feature	Audit Manager support
Identity-based policies	Yes
Resource-based policies	No
Policy actions	Yes
Policy resources	Yes
Policy condition keys	Partial
ACLs	No
ABAC (tags in policies)	Yes
Temporary credentials	Yes
Forward access sessions (FAS)	Yes
Service roles	No
Service-linked roles	Yes

To get a high-level view of how AWS Audit Manager and other AWS services work with most IAM features, see AWS services that work with IAM in the *IAM User Guide*.

Identity-based policies for AWS Audit Manager

Supports identity-based policies: Yes

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, group of users, or role. These policies control what actions users and roles can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see Define custom IAM permissions with customer managed policies in the *IAM User Guide*.

With IAM identity-based policies, you can specify allowed or denied actions and resources as well as the conditions under which actions are allowed or denied. You can't specify the principal in an identity-based policy because it applies to the user or role to which it is attached. To learn about all of the elements that you can use in a JSON policy, see IAM JSON policy elements reference in the *IAM User Guide*.

AWS Audit Manager creates a managed policy named `AWSAuditManagerAdministratorAccess` for Audit Manager administrators. This policy grants full administration access in Audit Manager. Administrators can attach this policy to any existing role or user, or create a new role with this policy.

Recommended policies for user personas in AWS Audit Manager

AWS Audit Manager enables you to maintain the segregation of duties among different users and for different audits by using different IAM policies. The two personas in Audit Manager and their recommended policies are defined as follows.

Persona	Description and recommended policy
Audit owner	• This persona must have the necessary permissions to manage assessments in AWS Audit Manager. • The recommended policy to use for this persona is the managed policy named AWSAuditManagerAdministratorAccess. You can use this policy as a starting point, and scope down these permissions as needed to fit your requirements.
Delegate	• This persona can access the delegated control sets in an assessment. They can update the control status, add comments, submit a control set for review, and add evidence to the assessment report. • The recommended policy to use for this persona is the following example policy: Allow users management access to AWS Audit Manager. You can use this

Persona	Description and recommended policy
	policy as a starting point, and make changes as necessary to fit your requirements.

Identity-based policy examples for AWS Audit Manager

To view examples of Audit Manager identity-based policies, see Identity-based policy examples for AWS Audit Manager.

Resource-based policies within AWS Audit Manager

Supports resource-based policies: No

Resource-based policies are JSON policy documents that you attach to a resource. Examples of resource-based policies are IAM *role trust policies* and Amazon S3 *bucket policies*. In services that support resource-based policies, service administrators can use them to control access to a specific resource. For the resource where the policy is attached, the policy defines what actions a specified principal can perform on that resource and under what conditions. You must specify a principal in a resource-based policy. Principals can include accounts, users, roles, federated users, or AWS services.

To enable cross-account access, you can specify an entire account or IAM entities in another account as the principal in a resource-based policy. Adding a cross-account principal to a resource-based policy is only half of establishing the trust relationship. When the principal and the resource are in different AWS accounts, an IAM administrator in the trusted account must also grant the principal entity (user or role) permission to access the resource. They grant permission by attaching an identity-based policy to the entity. However, if a resource-based policy grants access to a principal in the same account, no additional identity-based policy is required. For more information, see Cross account resource access in IAM in the *IAM User Guide*.

Although AWS Audit Manager does not allow you to manage resource-based policies through IAM, the service internally implements and manages resource-based policies for the following two scenarios:

- When audit owners are assigned to an assessment, a resource-based policy is attached to the assessment with the principal as the audit owner. For more information, see Step 3: Specify audit owners and Step 3: Edit audit owners.

- When a control set of an assessment is delegated, a resource-based policy is attached to the control set with the principal as the delegate. For more information, see Delegating a control set for review in AWS Audit Manager.

Policy actions for AWS Audit Manager

Supports policy actions: Yes

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Action` element of a JSON policy describes the actions that you can use to allow or deny access in a policy. Policy actions usually have the same name as the associated AWS API operation. There are some exceptions, such as *permission-only actions* that don't have a matching API operation. There are also some operations that require multiple actions in a policy. These additional actions are called *dependent actions*.

Include actions in a policy to grant permissions to perform the associated operation.

To see a list of AWS Audit Manager actions, see Actions defined by AWS Audit Manager in the *Service Authorization Reference*.

Policy actions in AWS Audit Manager use the following prefix before the action.

```
auditmanager
```

To specify multiple actions in a single statement, separate them with commas.

```
"Action": [
      "auditmanager:GetEvidenceDetails",
      "auditmanager:GetEvidenceEventDetails"
         ]
```

You can specify multiple actions using wildcards (*). For example, to specify all actions that begin with the word `Get`, include the following action.

```
"Action": "auditmanager:Get*"
```

To view examples of Audit Manager identity-based policies, see Identity-based policy examples for AWS Audit Manager.

Policy resources for AWS Audit Manager

Supports policy resources: Yes

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Resource` JSON policy element specifies the object or objects to which the action applies. Statements must include either a `Resource` or a `NotResource` element. As a best practice, specify a resource using its Amazon Resource Name (ARN). You can do this for actions that support a specific resource type, known as *resource-level permissions*.

For actions that don't support resource-level permissions, such as listing operations, use a wildcard (*) to indicate that the statement applies to all resources.

```
"Resource": "*"
```

To see a list of AWS Audit Manager resource types and their ARNs, see Resources defined by AWS Audit Manager in the *Service Authorization Reference*. To learn about actions with which you can specify the ARN of each resource, see Actions defined by AWS Audit Manager.

An Audit Manager assessment has the following Amazon Resource Name (ARN) format:

```
arn:${Partition}:auditmanager:${Region}:${Account}:assessment/${assessmentId}
```

An Audit Manager control set has the following ARN format:

```
arn:${Partition}:auditmanager:${Region}:${Account}:assessment/
${assessmentId}controlSet/${controlSetId}
```

An Audit Manager control has the following ARN format:

```
arn:${Partition}:auditmanager:${Region}:${Account}:control/${controlId}
```

For more information about the format of ARNs, see Amazon Resource Names (ARNs).

For example, to specify the `i-1234567890abcdef0` assessment in your statement, use the following ARN.

```
"Resource": "arn:aws:auditmanager:us-east-1:123456789012:assessment/
i-1234567890abcdef0"
```

To specify all instances that belong to a specific account, use the wildcard (*).

```
"Resource": "arn:aws:auditmanager:us-east-1:123456789012:assessment/*"
```

Some Audit Manager actions, such as those for creating resources, cannot be performed on a specific resource. In those cases, you must use the wildcard (*).

```
"Resource": "*"
```

Many Audit Manager API actions involve multiple resources. For example, `ListAssessments` returns a list of assessment metadata that's accessible by the currently logged in AWS account. Therefore, a user must have permissions to view the assessments. To specify multiple resources in a single statement, separate the ARNs with commas.

```
"Resource": [
      "resource1",
      "resource2"
```

To see a list of Audit Manager resource types and their ARNs, see Resources Defined by AWS Audit Manager in the *IAM User Guide*. To learn about actions with which you can specify the ARN of each resource, see Actions Defined by AWS Audit Manager.

Some Audit Manager API actions support multiple resources. For example, `GetChangeLogs` accesses an `assessmentID`, `controlID`, and `controlSetId`, so a principal must have permissions to access each of these resources. To specify multiple resources in a single statement, separate the ARNs with commas.

```
"Resource": [
      "assessmentId",
      "controlId",
```

```
        "controlSetId"
```

Policy condition keys for AWS Audit Manager

Supports service-specific policy condition keys: Partial

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Condition` element (or `Condition` *block*) lets you specify conditions in which a statement is in effect. The `Condition` element is optional. You can create conditional expressions that use condition operators, such as equals or less than, to match the condition in the policy with values in the request.

If you specify multiple `Condition` elements in a statement, or multiple keys in a single `Condition` element, AWS evaluates them using a logical `AND` operation. If you specify multiple values for a single condition key, AWS evaluates the condition using a logical `OR` operation. All of the conditions must be met before the statement's permissions are granted.

When the principal in a policy statement is an AWS service principal, we strongly recommend that you use the `aws:SourceArn` or `aws:SourceAccount` global condition keys in the policy. You can use these global condition context keys to help prevent the confused deputy scenario. The following documented policies show how you can use the `aws:SourceArn` and `aws:SourceAccount` global condition context keys in Audit Manager to prevent the confused deputy problem.

- Example policy for an SNS topic that's used for Audit Manager notifications
- Example policy for a KMS key that's used with an SNS topic

You can also use placeholder variables when you specify conditions. For example, you can grant a user permission to access a resource only if it is tagged with their user name. For more information, see IAM policy elements: variables and tags in the *IAM User Guide*.

Audit Manager does not provide any service-specific condition keys, but it does support using some global condition keys. To see all AWS global condition keys, see AWS global condition context keys in the *IAM User Guide*.

Access control lists (ACLs) in AWS Audit Manager

Supports ACLs: No

Access control lists (ACLs) control which principals (account members, users, or roles) have permissions to access a resource. ACLs are similar to resource-based policies, although they do not use the JSON policy document format.

Attribute-based access control (ABAC) with AWS Audit Manager

Supports ABAC (tags in policies): Yes

Attribute-based access control (ABAC) is an authorization strategy that defines permissions based on attributes. In AWS, these attributes are called *tags*. You can attach tags to IAM entities (users or roles) and to many AWS resources. Tagging entities and resources is the first step of ABAC. Then you design ABAC policies to allow operations when the principal's tag matches the tag on the resource that they are trying to access.

ABAC is helpful in environments that are growing rapidly and helps with situations where policy management becomes cumbersome.

To control access based on tags, you provide tag information in the condition element of a policy using the `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, or `aws:TagKeys` condition keys.

If a service supports all three condition keys for every resource type, then the value is **Yes** for the service. If a service supports all three condition keys for only some resource types, then the value is **Partial**.

For more information about ABAC, see Define permissions with ABAC authorization in the *IAM User Guide*. To view a tutorial with steps for setting up ABAC, see Use attribute-based access control (ABAC) in the *IAM User Guide*.

For more information about tagging AWS Audit Manager resources, see Tagging AWS Audit Manager resources.

Using temporary credentials with AWS Audit Manager

Supports temporary credentials: Yes

Some AWS services don't work when you sign in using temporary credentials. For additional information, including which AWS services work with temporary credentials, see AWS services that work with IAM in the *IAM User Guide*.

You are using temporary credentials if you sign in to the AWS Management Console using any method except a user name and password. For example, when you access AWS using your

company's single sign-on (SSO) link, that process automatically creates temporary credentials. You also automatically create temporary credentials when you sign in to the console as a user and then switch roles. For more information about switching roles, see Switch from a user to an IAM role (console) in the *IAM User Guide*.

You can manually create temporary credentials using the AWS CLI or AWS API. You can then use those temporary credentials to access AWS. AWS recommends that you dynamically generate temporary credentials instead of using long-term access keys. For more information, see Temporary security credentials in IAM.

Forward access sessions for AWS Audit Manager

Supports forward access sessions (FAS): Yes

When you use an IAM user or role to perform actions in AWS, you are considered a principal. When you use some services, you might perform an action that then initiates another action in a different service. FAS uses the permissions of the principal calling an AWS service, combined with the requesting AWS service to make requests to downstream services. FAS requests are only made when a service receives a request that requires interactions with other AWS services or resources to complete. In this case, you must have permissions to perform both actions. For policy details when making FAS requests, see Forward access sessions.

Service roles for AWS Audit Manager

Supports service roles: No

A service role is an IAM role that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see Create a role to delegate permissions to an AWS service in the *IAM User Guide*.

> **Warning**
>
> Changing the permissions for a service role might break AWS Audit Manager functionality. Edit service roles only when Audit Manager provides guidance to do so.

Service-linked roles for AWS Audit Manager

Supports service-linked roles: Yes

A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your AWS account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.

For details about service-linked roles for AWS Audit Manager, see Using service-linked roles for AWS Audit Manager.

Identity-based policy examples for AWS Audit Manager

By default, users and roles don't have permission to create or modify Audit Manager resources. They also can't perform tasks by using the AWS Management Console, AWS Command Line Interface (AWS CLI), or AWS API. To grant users permission to perform actions on the resources that they need, an IAM administrator can create IAM policies. The administrator can then add the IAM policies to roles, and users can assume the roles.

To learn how to create an IAM identity-based policy by using these example JSON policy documents, see Create IAM policies (console) in the *IAM User Guide*.

For details about actions and resource types defined by AWS Audit Manager, including the format of the ARNs for each of the resource types, see Actions, resources, and condition keys for AWS Audit Manager in the *Service Authorization Reference*.

Contents

- Example 2 (Permissions for the KMS key that's attached to the SNS topic)
- Allow users to run search queries in evidence finder

Policy best practices

Identity-based policies determine whether someone can create, access, or delete Audit Manager resources in your account. These actions can incur costs for your AWS account. When you create or edit identity-based policies, follow these guidelines and recommendations:

- **Get started with AWS managed policies and move toward least-privilege permissions** – To get started granting permissions to your users and workloads, use the *AWS managed policies* that grant permissions for many common use cases. They are available in your AWS account. We recommend that you reduce permissions further by defining AWS customer managed policies that are specific to your use cases. For more information, see AWS managed policies or AWS managed policies for job functions in the *IAM User Guide*.
- **Apply least-privilege permissions** – When you set permissions with IAM policies, grant only the permissions required to perform a task. You do this by defining the actions that can be taken on specific resources under specific conditions, also known as *least-privilege permissions*. For more information about using IAM to apply permissions, see Policies and permissions in IAM in the *IAM User Guide*.
- **Use conditions in IAM policies to further restrict access** – You can add a condition to your policies to limit access to actions and resources. For example, you can write a policy condition to specify that all requests must be sent using SSL. You can also use conditions to grant access to service actions if they are used through a specific AWS service, such as AWS CloudFormation. For more information, see IAM JSON policy elements: Condition in the *IAM User Guide*.
- **Use IAM Access Analyzer to validate your IAM policies to ensure secure and functional permissions** – IAM Access Analyzer validates new and existing policies so that the policies adhere to the IAM policy language (JSON) and IAM best practices. IAM Access Analyzer provides more than 100 policy checks and actionable recommendations to help you author secure and functional policies. For more information, see Validate policies with IAM Access Analyzer in the *IAM User Guide*.
- **Require multi-factor authentication (MFA)** – If you have a scenario that requires IAM users or a root user in your AWS account, turn on MFA for additional security. To require MFA when API operations are called, add MFA conditions to your policies. For more information, see Secure API access with MFA in the *IAM User Guide*.

For more information about best practices in IAM, see Security best practices in IAM in the *IAM User Guide*.

Allow the minimum permissions required to enable Audit Manager

This example shows how you might allow accounts without an administrator role to enable AWS Audit Manager.

> **Note**
>
> What we provide here is a basic policy that grants the minimum permissions needed to enable Audit Manager. All of the permissions in the following policy are required. If you omit any part of this policy, you won't be able to enable Audit Manager.
> We recommend that you take time to customize your permissions so they meet your specific needs. If you need help, contact your administrator or AWS Support.

To grant the minimum access required to enable Audit Manager, use the following permissions.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "auditmanager:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        },
        {
            "Sid": "CreateEventsAccess",
```

```
            "Effect": "Allow",
            "Action": [
                "events:PutRule"
            ],
            "Resource": "*",
            "Condition": {
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.securityhub"
                    ]
                }
            }
        },
        {
            "Sid": "EventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/
AuditManagerSecurityHubFindingsReceiver"
        },
        {
            "Effect": "Allow",
            "Action": "kms:ListAliases",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        }
    ]
}
```

You don't need to allow minimum console permissions for users that are making calls only to the AWS CLI or the AWS API. Instead, allow access to only the actions that match the API operation that you're trying to perform.

Allow users full administrator access to AWS Audit Manager

The following example policies grant full administrator access to AWS Audit Manager.

- Example 1 (Managed policy, AWSAuditManagerAdministratorAccess)
- Example 2 (Assessment report destination permissions)
- Example 3 (Permissions to enable evidence finder)
- Example 4 (Permissions to disable evidence finder)

Example 1 (Managed policy, AWSAuditManagerAdministratorAccess)

The AWSAuditManagerAdministratorAccess policy includes the ability to enable and disable Audit Manager, the ability to change Audit Manager settings, and the ability to manage all Audit Manager resources such as assessments, frameworks, controls, and assessment reports.

Example 2 (Assessment report destination permissions)

This policy grants you permission to access a specific S3 bucket, and to add files to and delete files from it. This allows you to use the specified bucket as an assessment report destination in Audit Manager.

Replace the *placeholder text* with your own information. Include the S3 bucket that you use as your assessment report destination and the KMS key that you use to encrypt your assessment reports.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:DeleteObject",
        "s3:GetBucketLocation",
        "s3:PutObjectAcl"
      ],
      "Resource": "arn:aws:s3:::example-s3-destination-bucket/*"
    },
    {
      "Effect": "Allow",
```

```
      "Action": [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "arn:aws:kms:us-
west-2:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }
  ]
}
```

Example 3 (Permissions to enable evidence finder)

The following permission policy is required if you want to enable and use the evidence finder feature. This policy statement allows Audit Manager to create a CloudTrail Lake event data store and run search queries.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
           "Sid": "ManageCloudTrailLakeQueryAccess",
           "Effect": "Allow",
           "Action": [
               "cloudtrail:StartQuery",
               "cloudtrail:DescribeQuery",
               "cloudtrail:GetQueryResults",
               "cloudtrail:CancelQuery"
           ],
           "Resource": "arn:aws:cloudtrail:*:*:eventdatastore/*"
        },
        {
           "Sid": "ManageCloudTrailLakeAccess",
           "Effect": "Allow",
           "Action": [
                "cloudtrail:CreateEventDataStore"
           ],
           "Resource": "arn:aws:cloudtrail:*:*:eventdatastore/*"
         }
```

```
    ]
}
```

Example 4 (Permissions to disable evidence finder)

This example policy grants permission to disable the evidence finder feature in Audit Manager. This involves deleting the event data store that was created when you first enabled the feature.

Before you use this policy, replace the *placeholder text* with your own information. You should specify the UUID of the event data store that was created when you enabled evidence finder. You can retrieve the ARN of the event data store from your Audit Manager settings. For more information, see GetSettings in the *AWS Audit Manager API Reference*.

Allow users management access to AWS Audit Manager

This example shows how you might allow non-administrator management access to AWS Audit Manager.

This policy grants the ability to manage all Audit Manager resources (assessments, frameworks, and controls), but does not grant the ability to enable or disable Audit Manager or to modify Audit Manager settings.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:AssociateAssessmentReportEvidenceFolder",
                "auditmanager:BatchAssociateAssessmentReportEvidence",
                "auditmanager:BatchCreateDelegationByAssessment",
                "auditmanager:BatchDeleteDelegationByAssessment",
                "auditmanager:BatchDisassociateAssessmentReportEvidence",
                "auditmanager:BatchImportEvidenceToAssessmentControl",
                "auditmanager:CreateAssessment",
                "auditmanager:CreateAssessmentFramework",
                "auditmanager:CreateAssessmentReport",
                "auditmanager:CreateControl",
```

```
                "auditmanager:DeleteControl",
                "auditmanager:DeleteAssessment",
                "auditmanager:DeleteAssessmentFramework",
                "auditmanager:DeleteAssessmentFrameworkShare",
                "auditmanager:DeleteAssessmentReport",
                "auditmanager:DisassociateAssessmentReportEvidenceFolder",
                "auditmanager:GetAccountStatus",
                "auditmanager:GetAssessment",
                "auditmanager:GetAssessmentFramework",
                "auditmanager:GetControl",
                "auditmanager:GetServicesInScope",
                "auditmanager:GetSettings",
                "auditmanager:GetAssessmentReportUrl",
                "auditmanager:GetChangeLogs",
                "auditmanager:GetDelegations",
                "auditmanager:GetEvidence",
                "auditmanager:GetEvidenceByEvidenceFolder",
                "auditmanager:GetEvidenceFileUploadUrl",
                "auditmanager:GetEvidenceFolder",
                "auditmanager:GetEvidenceFoldersByAssessment",
                "auditmanager:GetEvidenceFoldersByAssessmentControl",
                "auditmanager:GetInsights",
                "auditmanager:GetInsightsByAssessment",
                "auditmanager:GetOrganizationAdminAccount",
                "auditmanager:ListAssessments",
                "auditmanager:ListAssessmentReports",
                "auditmanager:ListControls",
                "auditmanager:ListKeywordsForDataSource",
                "auditmanager:ListNotifications",
                "auditmanager:ListAssessmentControlInsightsByControlDomain",
                "auditmanager:ListAssessmentFrameworks",
                "auditmanager:ListAssessmentFrameworkShareRequests",
                "auditmanager:ListControlDomainInsights",
                "auditmanager:ListControlDomainInsightsByAssessment",
                "auditmanager:ListControlInsightsByControlDomain",
                "auditmanager:ListTagsForResource",
                "auditmanager:StartAssessmentFrameworkShare",
                "auditmanager:TagResource",
                "auditmanager:UntagResource",
                "auditmanager:UpdateControl",
                "auditmanager:UpdateAssessment",
                "auditmanager:UpdateAssessmentControl",
                "auditmanager:UpdateAssessmentControlSetStatus",
                "auditmanager:UpdateAssessmentFramework",
```

```
                "auditmanager:UpdateAssessmentFrameworkShare",
                "auditmanager:UpdateAssessmentStatus",
                "auditmanager:ValidateAssessmentReportIntegrity"
            ],
            "Resource": "*"
        },
        {
    "Sid": "ControlCatalogAccess",
    "Effect": "Allow",
    "Action": [
"controlcatalog:ListCommonControls",
"controlcatalog:ListDomains",
"controlcatalog:ListObjectives"
    ],
    "Resource": "*"
        },
        {
            "Sid": "OrganizationsAccess",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMAccess",
            "Effect": "Allow",
            "Action": [
                "iam:GetUser",
                "iam:ListUsers",
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "S3Access",
            "Effect": "Allow",
            "Action": [
```

```
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsAccess",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SNSAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Sid": "TagAccess",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        }
    ]
}
```

Allow users read-only access to AWS Audit Manager

This policy grants read-only access to AWS Audit Manager resources such as assessments, frameworks, and controls.

JSON

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:Get*",
                "auditmanager:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

Allow users to view their own permissions

This example shows how you might create a policy that allows IAM users to view the inline and managed policies that are attached to their user identity. This policy includes permissions to complete this action on the console or programmatically using the AWS CLI or AWS API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
```

```
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Allow AWS Audit Manager to send notifications to Amazon SNS topics

The policies in this example grant Audit Manager permissions to send notifications to an existing Amazon SNS topic.

- Example 1 – If you want to receive notifications from Audit Manager, use this example to add permissions to your SNS topic access policy.
- Example 2 – If your SNS topic uses AWS Key Management Service (AWS KMS) for server-side encryption (SSE), use this example to add permissions to the KMS key access policy.

In the following policies, the principal who gets the permissions is the Audit Manager service principal, which is `auditmanager.amazonaws.com`. When the principal in a policy statement is an AWS service principal, we strongly recommend that you use the `aws:SourceArn` or `aws:SourceAccount` global condition keys in the policy. You can use these global condition context keys to help prevent the confused deputy scenario.

Example 1 (Permissions for the SNS topic)

This policy statement allows Audit Manager to publish events to the specified SNS topic. Any request to publish to the specified SNS topic must satisfy the policy conditions.

Before using this policy, replace the *`placeholder text`* with your own information. Take note of the following:

- If you use the `aws:SourceArn` condition key in this policy, the value must be the ARN of the Audit Manager resource that the notification comes from. In the example below, `aws:SourceArn` uses a wildcard (*) for the resource ID. This allows all requests that come from Audit Manager on all Audit Manager resources. With the `aws:SourceArn` global condition key,

you can use either the `StringLike` or the `ArnLike` condition operator. As a best practice, we recommend that you use `ArnLike`.

- If you use the `aws:SourceAccount` condition key, you can use either the `StringEquals` or the `StringLike` condition operator. As a best practice, we recommend that you use `StringEquals` to implement least privilege.
- If you use both `aws:SourceAccount` and `aws:SourceArn`, the account values must show the same account ID.

The following alternative example uses just the `aws:SourceArn` condition key, with the `StringLike` condition operator:

```
    "Condition": {
      "StringLike": {
        "aws:SourceArn": "arn:aws:auditmanager:region:accountID:*"
      }
    }
```

The following alternative example uses just the `aws:SourceAccount` condition key, with the `StringLike` condition operator:

```
  "Condition": {
    "StringLike": {
      "aws:SourceAccount": "accountID"
    }
  }
```

Example 2 (Permissions for the KMS key that's attached to the SNS topic)

This policy statement allows Audit Manager to use the KMS key to generate the data key that it uses to encrypt an SNS topic. Any request to use the KMS key for the specified operation must satisfy the policy conditions.

Before using this policy, replace the *placeholder text* with your own information. Take note of the following:

- If you use the `aws:SourceArn` condition key in this policy, the value must be the ARN of the resource that's being encrypted. For example, in this case, it's the SNS topic in your account. Set the value to the ARN or an ARN pattern with wildcard characters (*). You can use either the

`StringLike` or the `ArnLike` condition operator with the `aws:SourceArn` condition key. As a best practice, we recommend that you use `ArnLike`.

- If you use the `aws:SourceAccount` condition key, you can use either the `StringEquals` or the `StringLike` condition operator. As a best practice, we recommend that you use `StringEquals` to implement least privilege. You can use `aws:SourceAccount` if you don't know the ARN of the SNS topic.
- If you use both `aws:SourceAccount` and `aws:SourceArn`, the account values must show the same account ID.

The following alternative example uses just the `aws:SourceArn` condition key, with the `StringLike` condition operator:

```
    "Condition": {
      "StringLike": {
        "aws:SourceArn": "arn:aws:sns:region:accountID:topicName"
      }
    }
```

The following alternative example uses just the `aws:SourceAccount` condition key, with the `StringLike` condition operator:

```
  "Condition": {
    "StringLike": {
      "aws:SourceAccount": "accountID"
    }
   }
```

Allow users to run search queries in evidence finder

The following policy grants permissions to perform queries on a CloudTrail Lake event data store. This permission policy is required if you want to use the evidence finder feature.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "ManageCloudTrailLakeQueryAccess",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:StartQuery",
                "cloudtrail:DescribeQuery",
                "cloudtrail:GetQueryResults",
                "cloudtrail:CancelQuery"
            ],
            "Resource": "*"
        }
    ]
}
```

Cross-service confused deputy prevention

The confused deputy problem is a security issue where an entity that doesn't have permission to perform an action can coerce a more-privileged entity to perform the action. In AWS, cross-service impersonation can result in the confused deputy problem. Cross-service impersonation can occur when one service (the *calling service*) calls another service (the *called service*). The calling service can be manipulated to use its permissions to act on another customer's resources when it doesn't have permission to do so. To prevent this, Amazon Web Services provides tools that help you protect your data for all services with service principals that have been given access to resources in your account.

We recommend using the `aws:SourceArn` and `aws:SourceAccount` global condition context keys in resource policies to limit the permissions that AWS Audit Manager gives to another service for access to your resources.

- Use `aws:SourceArn` if you want only one resource to be associated with the cross-service access. You can also use `aws:SourceArn` with a wildcard (*) if you want to specify multiple resources.

  For example, you might use an Amazon SNS topic to receive activity notifications from Audit Manager. In this case, in your SNS topic access policy, the ARN value of `aws:SourceArn` is the Audit Manager resource that the notification comes from. Because it's likely that you have multiple Audit Manager resources, we recommend that you use `aws:SourceArn` with a wildcard. This enables you to specify all of your Audit Manager resources in your SNS topic access policy.

- Use `aws:SourceAccount` if you want to allow any resource in that account to be associated with the cross-service use.
- If the `aws:SourceArn` value doesn't contain the account ID, such as an Amazon S3 bucket ARN, you must use both global condition context keys to limit permissions.
- If you use both conditions, and if the `aws:SourceArn` value contains the account ID, the `aws:SourceAccount` value and the account in the `aws:SourceArn` value must show the same account ID when used in the same policy statement.
- The most effective way to protect against the confused deputy problem is to use the `aws:SourceArn` global condition context key with the full ARN of the resource. If you don't know the full Amazon Resource Name (ARN) of the resource or if you are specifying multiple resources, use the `aws:SourceArn` global context condition key with wildcard characters (*) for the unknown portions of the ARN. For example, `arn:aws:servicename:*:123456789012:*`.

Audit Manager confused deputy support

Audit Manager provides confused deputy support in the following scenarios. These policy examples show how you can use the `aws:SourceArn` and `aws:SourceAccount` condition keys to prevent the confused deputy problem.

- Example policy: The SNS topic that you use to receive Audit Manager notifications
- Example policy: The KMS key that you use to encrypt your SNS topic

Audit Manager doesn't provide confused deputy support for the customer managed key that you provide in your Audit Manager Configuring your data encryption settings settings. If you provided your own customer managed key, you can't use `aws:SourceAccount` or `aws:SourceArn` conditions in that KMS key policy.

Resource-based policy examples for AWS Audit Manager

Amazon S3 bucket policy

The following policy allows CloudTrail to deliver evidence finder query results to the specified S3 bucket. As a security best practice, the IAM global condition key `aws:SourceArn` helps ensure that CloudTrail writes to the S3 bucket only for the event data store.

Important

You must specify an S3 bucket for CloudTrail Lake query results delivery. For more information, see Specifying an existing bucket for CloudTrail Lake query results .

Replace the *placeholder text* with your own information, as follows:

- Replace *amzn-s3-demo-destination-bucket* with the S3 bucket that you use as your export destination.
- Replace *myQueryRunningRegion* with the appropriate AWS Region for your configuration.
- Replace *myAccountID* with the AWS account ID that's used for CloudTrail. This might not be the same as the AWS account ID for the S3 bucket. If this is an organization event data store, you must use the AWS account for the management account.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "s3:PutObject*",
                "s3:Abort*"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-destination-bucket",
                "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
            }
```

```
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
            }
        }
    ]
    }
```

AWS Key Management Service policy

If your S3 bucket has the default encryption set to SSE-KMS, grant access to CloudTrail in your AWS Key Management Service key's resource policy so it can use the key. In this case, add the following resource policy to the AWS KMS key.

JSON

```
{
 "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt*",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        },
        {
```

```
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt*",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS managed policies for AWS Audit Manager

An AWS managed policy is a standalone policy that is created and administered by AWS. AWS managed policies are designed to provide permissions for many common use cases so that you can start assigning permissions to users, groups, and roles.

Keep in mind that AWS managed policies might not grant least-privilege permissions for your specific use cases because they're available for all AWS customers to use. We recommend that you reduce permissions further by defining customer managed policies that are specific to your use cases.

You cannot change the permissions defined in AWS managed policies. If AWS updates the permissions defined in an AWS managed policy, the update affects all principal identities (users, groups, and roles) that the policy is attached to. AWS is most likely to update an AWS managed policy when a new AWS service is launched or new API operations become available for existing services.

For more information, see AWS managed policies in the *IAM User Guide*.

Topics

- AWS managed policy: AWSAuditManagerAdministratorAccess
- AWS managed policy: AWSAuditManagerServiceRolePolicy
- AWS Audit Manager updates to AWS managed policies

AWS managed policy: AWSAuditManagerAdministratorAccess

You can attach the `AWSAuditManagerAdministratorAccess` policy to your IAM identities.

This policy grants administrative permissions that allow full administration access to AWS Audit Manager. This access includes the ability to enable and disable AWS Audit Manager, change settings in AWS Audit Manager, and manage all Audit Manager resources such as assessments, frameworks, controls, and assessment reports.

AWS Audit Manager requires broad permissions across multiple AWS services. This is because AWS Audit Manager integrates with multiple AWS services to collect evidence automatically from the AWS account and services in scope of an assessment.

Permissions details

This policy includes the following permissions:

- `Audit Manager` – Allows principals full permissions on AWS Audit Manager resources.
- `Organizations` – Allows principals to list accounts and organizational units, and to register or deregister a delegated administrator. This is required so that you can enable multi-account support and allow AWS Audit Manager to run assessments over multiple accounts and consolidate evidence into a delegated administrator account.
- `iam` – Allows principals to get and list users in IAM and create a service-linked role. This is required so that you can designate audit owners and delegates for an assessment. This policy also allows principals to delete the service-linked role and retrieve the deletion status. This is required so that AWS Audit Manager can clean up resources and delete the service-linked role for you when you choose to disable the service in the AWS Management Console.
- `s3` – Allows principals to list available Amazon Simple Storage Service (Amazon S3) buckets. This capability is required so that you can designate the S3 bucket in which you want to store evidence reports or upload manual evidence.
- `kms` – Allows principals to list and describe keys, list aliases, and create grants. This is required so that you can choose customer managed keys for data encryption.
- `sns` – Allows principals to list subscription topics in Amazon SNS. This is required so that you can specify which SNS topic you want AWS Audit Manager to send notifications to.
- `events` – Allows principals to list and manage checks from AWS Security Hub. This is required so that AWS Audit Manager can automatically collect AWS Security Hub findings for the AWS services that are monitored by AWS Security Hub. It can then convert this data into evidence to be included in your AWS Audit Manager assessments.

- `tag` – Allows principals to retrieve tagged resources. This is required so that you can use tags as a search filter when browsing frameworks, controls, and assessments in AWS Audit Manager.
- `controlcatalog` – Allows principals to list the domains, objectives, and common controls that are provided by AWS Control Catalog. This is required so that you can use the common controls feature in AWS Audit Manager. With these permissions in place, you can view a list of common controls in the AWS Audit Manager control library, and filter controls by domain and objective. You can also use common controls as an evidence source when you create a custom control.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "OrganizationsAccess",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowOnlyAuditManagerIntegration",
            "Effect": "Allow",
            "Action": [
                "organizations:RegisterDelegatedAdministrator",
                "organizations:DeregisterDelegatedAdministrator",
```

```
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:ServicePrincipal": [
                        "auditmanager.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "IAMAccess",
            "Effect": "Allow",
            "Action": [
                "iam:GetUser",
                "iam:ListUsers",
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMAccessCreateSLR",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        },
        {
            "Sid": "IAMAccessManageSLR",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteServiceLinkedRole",
                "iam:UpdateRoleDescription",
                "iam:GetServiceLinkedRoleDeletionStatus"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*"
        },
```

```
        {
            "Sid": "S3Access",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsAccess",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsCreateGrantAccess",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                },
                "StringLike": {
                    "kms:ViaService": "auditmanager.*.amazonaws.com"
                }
            }
        },
        {
            "Sid": "SNSAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateEventsAccess",
```

```
            "Effect": "Allow",
            "Action": [
                "events:PutRule"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "events:detail-type": "Security Hub Findings - Imported"
                },
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.securityhub"
                    ]
                }
            }
        },
        {
            "Sid": "EventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:DeleteRule",
                "events:DescribeRule",
                "events:EnableRule",
                "events:DisableRule",
                "events:ListTargetsByRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/
AuditManagerSecurityHubFindingsReceiver"
        },
        {
            "Sid": "TagAccess",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        },
        {
     "Sid": "ControlCatalogAccess",
     "Effect": "Allow",
     "Action": [
  "controlcatalog:ListCommonControls",
```

```
  "controlcatalog:ListDomains",
  "controlcatalog:ListObjectives"
     ],
     "Resource": "*"
        }
    ]
}
```

AWS managed policy: AWSAuditManagerServiceRolePolicy

You can't attach `AWSAuditManagerServiceRolePolicy` to your IAM entities. This policy is attached to a service-linked role, `AWSServiceRoleForAuditManager`, that allows AWS Audit Manager to perform actions on your behalf. For more information, see Using service-linked roles for AWS Audit Manager.

The role permissions policy, `AWSAuditManagerServiceRolePolicy`, allows AWS Audit Manager to collect automated evidence by doing the following on your behalf:

- Collect data from the following data sources:
  - Management events from AWS CloudTrail
  - Compliance checks from AWS Config Rules
  - Compliance checks from AWS Security Hub
- Use API calls to describe your resource configurations for the following AWS services.

> **Tip**
>
> For more information about the API calls that Audit Manager uses to collect evidence from these services, see Supported API calls for custom control data sources in this guide.

  - Amazon API Gateway
  - AWS Backup
  - Amazon Bedrock
  - AWS Certificate Manager
  - Amazon CloudFront
  - AWS CloudTrail

- Amazon CloudWatch
- Amazon CloudWatch Logs
- Amazon Cognito user pools
- AWS Config
- Amazon Data Firehose
- AWS Direct Connect
- Amazon DynamoDB
- Amazon EC2
- Amazon EC2 Auto Scaling
- Amazon Elastic Container Service
- Amazon Elastic File System
- Amazon Elastic Kubernetes Service
- Amazon ElastiCache
- Elastic Load Balancing
- Amazon EMR
- Amazon EventBridge
- Amazon FSx
- Amazon GuardDuty
- AWS Identity and Access Management (IAM)
- Amazon Kinesis
- AWS KMS
- AWS Lambda
- AWS License Manager
- Amazon Managed Streaming for Apache Kafka
- Amazon OpenSearch Service
- AWS Organizations
- Amazon Relational Database Service
- Amazon Redshift
- Amazon Route 53

- Amazon S3

- Amazon SageMaker AI
- AWS Secrets Manager
- AWS Security Hub
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- AWS WAF

Permissions details

`AWSAuditManagerServiceRolePolicy` allows AWS Audit Manager to complete the following actions on the specified resources:

- `acm:GetAccountConfiguration`
- `acm:ListCertificates`
- `apigateway:GET`
- `autoscaling:DescribeAutoScalingGroups`
- `backup:ListBackupPlans`
- `backup:ListRecoveryPointsByResource`
- `bedrock:GetCustomModel`
- `bedrock:GetFoundationModel`
- `bedrock:GetModelCustomizationJob`
- `bedrock:GetModelInvocationLoggingConfiguration`
- `bedrock:ListCustomModels`
- `bedrock:ListFoundationModels`
- `bedrock:ListGuardrails`
- `bedrock:ListModelCustomizationJobs`
- `cloudfront:GetDistribution`
- `cloudfront:GetDistributionConfig`
- `cloudfront:ListDistributions`
- `cloudtrail:DescribeTrails`
- `cloudtrail:GetTrail`

- cloudtrail:ListTrails
- cloudtrail:LookupEvents
- cloudwatch:DescribeAlarms
- cloudwatch:DescribeAlarmsForMetric
- cloudwatch:GetMetricStatistics
- cloudwatch:ListMetrics
- cognito-idp:DescribeUserPool
- config:DescribeConfigRules
- config:DescribeDeliveryChannels
- config:ListDiscoveredResources
- directconnect:DescribeDirectConnectGateways
- directconnect:DescribeVirtualGateways
- dynamodb:DescribeBackup
- dynamodb:DescribeContinuousBackups
- dynamodb:DescribeTable
- dynamodb:DescribeTableReplicaAutoScaling
- dynamodb:ListBackups
- dynamodb:ListGlobalTables
- dynamodb:ListTables
- ec2:DescribeAddresses
- ec2:DescribeCustomerGateways
- ec2:DescribeEgressOnlyInternetGateways
- ec2:DescribeFlowLogs
- ec2:DescribeInstanceCreditSpecifications
- ec2:DescribeInstanceAttribute
- ec2:DescribeInstances
- ec2:DescribeInternetGateways
- ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations
- ec2:DescribeLocalGateways

- ec2:DescribeLocalGatewayVirtualInterfaces
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSecurityGroupRules
- ec2:DescribeSnapshots
- ec2:DescribeTransitGateways
- ec2:DescribeVolumes
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcEndpointConnections
- ec2:DescribeVpcEndpointServiceConfigurations
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DescribeVpnConnections
- ec2:DescribeVpnGateways
- ec2:GetEbsDefaultKmsKeyId
- ec2:GetEbsEncryptionByDefault
- ec2:GetLaunchTemplateData
- ecs:DescribeClusters
- eks:DescribeAddonVersions
- elasticache:DescribeCacheClusters
- elasticache:DescribeServiceUpdates
- elasticfilesystem:DescribeAccessPoints
- elasticfilesystem:DescribeFileSystems
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeSslPolicies
- elasticloadbalancing:DescribeTargetGroups
- elasticmapreduce:ListClusters

- elasticmapreduce:ListSecurityConfigurations
- es:DescribeDomains
- es:DescribeDomain
- es:DescribeDomainConfig
- es:ListDomainNames
- events:DeleteRule
- events:DescribeRule
- events:DisableRule
- events:EnableRule
- events:ListConnections
- events:ListEventBuses
- events:ListEventSources
- events:ListRules
- events:ListTargetsByRule
- events:PutRule
- events:PutTargets
- events:RemoveTargets
- firehose:ListDeliveryStreams
- fsx:DescribeFileSystems
- guardduty:ListDetectors
- iam:GenerateCredentialReport
- iam:GetAccessKeyLastUsed
- iam:GetAccountAuthorizationDetails
- iam:GetAccountPasswordPolicy
- iam:GetAccountSummary
- iam:GetCredentialReport
- iam:GetGroupPolicy
- iam:GetPolicy
- iam:GetPolicyVersion

- iam:GetRolePolicy
- iam:GetUser
- iam:GetUserPolicy
- iam:ListAccessKeys
- iam:ListAttachedGroupPolicies
- iam:ListAttachedRolePolicies
- iam:ListAttachedUserPolicies
- iam:ListEntitiesForPolicy
- iam:ListGroupsForUser
- iam:ListGroupPolicies
- iam:ListGroups
- iam:ListMfaDeviceTags
- iam:ListMfaDevices
- iam:ListOpenIdConnectProviders
- iam:ListPolicies
- iam:ListPolicyVersions
- iam:ListRolePolicies
- iam:ListRoles
- iam:ListSamlProviders
- iam:ListUserPolicies
- iam:ListUsers
- iam:ListVirtualMFADevices
- kafka:ListClusters
- kafka:ListKafkaVersions
- kinesis:ListStreams
- kms:DescribeKey
- kms:GetKeyPolicy
- kms:GetKeyRotationStatus
- kms:ListGrants

- kms:ListKeyPolicies
- kms:ListKeys
- lambda:ListFunctions
- license-manager:ListAssociationsForLicenseConfiguration
- license-manager:ListLicenseConfigurations
- license-manager:ListUsageForLicenseConfiguration
- logs:DescribeDestinations
- logs:DescribeExportTasks
- logs:DescribeLogGroups
- logs:DescribeMetricFilters
- logs:DescribeResourcePolicies
- logs:FilterLogEvents
- logs:GetDataProtectionPolicy
- organizations:DescribeOrganization
- organizations:DescribePolicy
- rds:DescribeCertificates
- rds:DescribeDBClusterEndpoints
- rds:DescribeDBClusterParameterGroups
- rds:DescribeDBClusters
- rds:DescribeDBInstances
- rds:DescribeDBInstanceAutomatedBackups
- rds:DescribeDBSecurityGroups
- redshift:DescribeClusters
- redshift:DescribeClusterSnapshots
- redshift:DescribeLoggingStatus
- route53:GetQueryLoggingConfig
- s3:GetBucketAcl
- s3:GetBucketLogging

- s3:GetBucketOwnershipControls
- s3:GetBucketPolicy
  - This API action operates within the scope of the AWS account where the service-linked-role is available. It can't access cross-account bucket policies.
- s3:GetBucketPublicAccessBlock
- s3:GetBucketTagging
- s3:GetBucketVersioning
- s3:GetEncryptionConfiguration
- s3:GetLifecycleConfiguration
- s3:ListAllMyBuckets
- sagemaker:DescribeAlgorithm
- sagemaker:DescribeDomain
- sagemaker:DescribeEndpoint
- sagemaker:DescribeEndpointConfig
- sagemaker:DescribeFlowDefinition
- sagemaker:DescribeHumanTaskUi
- sagemaker:DescribeLabelingJob
- sagemaker:DescribeModel
- sagemaker:DescribeModelBiasJobDefinition
- sagemaker:DescribeModelCard
- sagemaker:DescribeModelQualityJobDefinition
- sagemaker:DescribeTrainingJob
- sagemaker:DescribeUserProfile
- sagemaker:ListAlgorithms
- sagemaker:ListDomains
- sagemaker:ListEndpointConfigs
- sagemaker:ListEndpoints
- sagemaker:ListFlowDefinitions
- sagemaker:ListHumanTaskUis

- sagemaker:ListLabelingJobs
- sagemaker:ListModels
- sagemaker:ListModelBiasJobDefinitions
- sagemaker:ListModelCards
- sagemaker:ListModelQualityJobDefinitions
- sagemaker:ListMonitoringAlerts
- sagemaker:ListMonitoringSchedules
- sagemaker:ListTrainingJobs
- sagemaker:ListUserProfiles
- securityhub:DescribeStandards
- secretsmanager:DescribeSecret
- secretsmanager:ListSecrets
- sns:ListTagsForResource
- sns:ListTopics
- sqs:ListQueues
- waf-regional:GetLoggingConfiguration
- waf-regional:GetRule
- waf-regional:GetWebAcl
- waf-regional:ListRuleGroups
- waf-regional:ListRules
- waf-regional:ListSubscribedRuleGroups
- waf-regional:ListWebACLs
- waf:GetRule
- waf:GetRuleGroup
- waf:ListActivatedRulesInRuleGroup
- waf:ListRuleGroups
- waf:ListRules
- waf:ListWebAcls
- wafv2:ListWebAcls

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "acm:GetAccountConfiguration",
    "acm:ListCertificates",
    "autoscaling:DescribeAutoScalingGroups",
    "backup:ListBackupPlans",
    "backup:ListRecoveryPointsByResource",
    "bedrock:GetCustomModel",
    "bedrock:GetFoundationModel",
    "bedrock:GetModelCustomizationJob",
    "bedrock:GetModelInvocationLoggingConfiguration",
    "bedrock:ListCustomModels",
    "bedrock:ListFoundationModels",
    "bedrock:ListGuardrails",
    "bedrock:ListModelCustomizationJobs",
    "cloudfront:GetDistribution",
    "cloudfront:GetDistributionConfig",
    "cloudfront:ListDistributions",
    "cloudtrail:GetTrail",
    "cloudtrail:ListTrails",
    "cloudtrail:DescribeTrails",
    "cloudtrail:LookupEvents",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:DescribeAlarmsForMetric",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "cognito-idp:DescribeUserPool",
    "config:DescribeConfigRules",
    "config:DescribeDeliveryChannels",
    "config:ListDiscoveredResources",
    "directconnect:DescribeDirectConnectGateways",
    "directconnect:DescribeVirtualGateways",
    "dynamodb:DescribeContinuousBackups",
    "dynamodb:DescribeBackup",
    "dynamodb:DescribeTableReplicaAutoScaling",
    "dynamodb:DescribeTable",
    "dynamodb:ListBackups",
```

```
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTables",
        "ec2:DescribeInstanceCreditSpecifications",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:GetLaunchTemplateData",
        "ec2:DescribeAddresses",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault",
        "ecs:DescribeClusters",
        "eks:DescribeAddonVersions",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeServiceUpdates",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeSslPolicies",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListSecurityConfigurations",
        "events:DescribeRule",
        "events:ListConnections",
```

```
        "events:ListEventBuses",
        "events:ListEventSources",
        "events:ListRules",
        "firehose:ListDeliveryStreams",
        "fsx:DescribeFileSystems",
        "guardduty:ListDetectors",
        "iam:GenerateCredentialReport",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetAccessKeyLastUsed",
        "iam:GetCredentialReport",
        "iam:GetGroupPolicy",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRolePolicy",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:ListAttachedGroupPolicies",
        "iam:ListAttachedUserPolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupsForUser",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListOpenIdConnectProviders",
        "iam:ListPolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSamlProviders",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "iam:ListPolicyVersions",
        "iam:ListAccessKeys",
        "iam:ListAttachedRolePolicies",
        "iam:ListMfaDeviceTags",
        "iam:ListMfaDevices",
        "kafka:ListClusters",
        "kafka:ListKafkaVersions",
        "kinesis:ListStreams",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListGrants",
```

```
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "lambda:ListFunctions",
        "license-manager:ListAssociationsForLicenseConfiguration",
        "license-manager:ListLicenseConfigurations",
        "license-manager:ListUsageForLicenseConfiguration",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeLogGroups",
        "logs:DescribeMetricFilters",
        "logs:DescribeResourcePolicies",
        "logs:FilterLogEvents",
        "logs:GetDataProtectionPolicy",
        "es:DescribeDomains",
        "es:DescribeDomain",
        "es:DescribeDomainConfig",
        "es:ListDomainNames",
        "organizations:DescribeOrganization",
        "organizations:DescribePolicy",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterEndpoints",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeLoggingStatus",
        "route53:GetQueryLoggingConfig",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelCard",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListAlgorithms",
```

```
      "sagemaker:ListDomains",
      "sagemaker:ListEndpoints",
      "sagemaker:ListEndpointConfigs",
      "sagemaker:ListFlowDefinitions",
      "sagemaker:ListHumanTaskUis",
      "sagemaker:ListLabelingJobs",
      "sagemaker:ListModels",
      "sagemaker:ListModelBiasJobDefinitions",
      "sagemaker:ListModelCards",
      "sagemaker:ListModelQualityJobDefinitions",
      "sagemaker:ListMonitoringAlerts",
      "sagemaker:ListMonitoringSchedules",
      "sagemaker:ListTrainingJobs",
      "sagemaker:ListUserProfiles",
      "s3:GetBucketPublicAccessBlock",
      "s3:GetBucketVersioning",
      "s3:GetEncryptionConfiguration",
      "s3:GetLifecycleConfiguration",
      "s3:ListAllMyBuckets",
      "secretsmanager:DescribeSecret",
      "secretsmanager:ListSecrets",
      "securityhub:DescribeStandards",
      "sns:ListTagsForResource",
      "sns:ListTopics",
      "sqs:ListQueues",
      "waf-regional:GetRule",
      "waf-regional:GetWebAcl",
      "waf:GetRule",
      "waf:GetRuleGroup",
      "waf:ListActivatedRulesInRuleGroup",
      "waf:ListWebAcls",
      "wafv2:ListWebAcls",
      "waf-regional:GetLoggingConfiguration",
      "waf-regional:ListRuleGroups",
      "waf-regional:ListSubscribedRuleGroups",
      "waf-regional:ListWebACLs",
      "waf-regional:ListRules",
      "waf:ListRuleGroups",
      "waf:ListRules"
    ],
    "Resource": "*",
    "Sid": "APIsAccess"
  },
  {
```

```
    "Sid": "S3Access",
    "Effect": "Allow",
    "Action": [
     "s3:GetBucketAcl",
     "s3:GetBucketLogging",
     "s3:GetBucketOwnershipControls",
     "s3:GetBucketPolicy",
     "s3:GetBucketTagging"
    ],
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": [
       "${aws:PrincipalAccount}"
      ]
     }
    }
   },
   {
    "Sid": "APIGatewayAccess",
    "Effect": "Allow",
    "Action": [
     "apigateway:GET"
    ],
    "Resource": [
     "arn:aws:apigateway:*::/restapis",
     "arn:aws:apigateway:*::/restapis/*/stages/*",
     "arn:aws:apigateway:*::/restapis/*/stages"
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": [
       "${aws:PrincipalAccount}"
      ]
     }
    }
   },
   {
    "Sid": "CreateEventsAccess",
    "Effect": "Allow",
    "Action": [
     "events:PutRule"
    ],
    "Resource": "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver",
```

```
    "Condition": {
     "StringEquals": {
      "events:detail-type": "Security Hub Findings - Imported"
     },
     "Null": {
      "events:source": "false"
     },
     "ForAllValues:StringEquals": {
      "events:source": [
       "aws.securityhub"
      ]
     }
    }
   },
   {
    "Sid": "EventsAccess",
    "Effect": "Allow",
    "Action": [
     "events:DeleteRule",
     "events:DescribeRule",
     "events:EnableRule",
     "events:DisableRule",
     "events:ListTargetsByRule",
     "events:PutTargets",
     "events:RemoveTargets"
    ],
    "Resource": "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
   }
  ]
}
```

AWS Audit Manager updates to AWS managed policies

View details about updates to AWS managed policies for AWS Audit Manager since this service began tracking these changes. For automatic alerts about changes to this page, subscribe to the RSS feed on the AWS Audit Manager Document history page.

Change	Description	Date
AWSAuditManagerServiceRolePolicy – Update to an existing policy	The service-linked role now allows AWS Audit Manager to perform the `bedrock:ListGuardrails` action. This API action is required to support the AWS Generative AI Best Practices Framework v2. It allows Audit Manager to collect automated evidence about the guardrails that are in place for your generative AI model data training data sets.	09/24/2024
AWSAuditManagerServiceRolePolicy – Update to an existing policy	We added the following permissions to `AWSAuditManagerServiceRolePolicy` . AWS Audit Manager can now perform the following actions to collect automated evidence about the resources in your AWS account. • `sagemaker:DescribeAlgorithm` • `sagemaker:DescribeDomain` • `sagemaker:DescribeEndpoint` • `sagemaker:DescribeFlowDefinition` • `sagemaker:DescribeHumanTaskUi` • `sagemaker:DescribeLabelingJob` • `sagemaker:DescribeModel` • `sagemaker:DescribeModelBiasJobDefinition` • `sagemaker:DescribeModelCard` • `sagemaker:DescribeModelQualityJobDefinition` • `sagemaker:DescribeTrainingJob` • `sagemaker:DescribeUserProfile`	06/10/2024

Change	Description	Date
	• sagemaker:ListAlgorithms • sagemaker:ListDomains • sagemaker:ListEndpoints • sagemaker:ListFlowDefinitions • sagemaker:ListHumanTaskUis • sagemaker:ListLabelingJobs • sagemaker:ListModels • sagemaker:ListModelBiasJobDefinitions • sagemaker:ListModelCards • sagemaker:ListModelQualityJobDefinitions • sagemaker:ListMonitoringAlerts • sagemaker:ListMonitoringSchedules • sagemaker:ListTrainingJobs • sagemaker:ListUserProfiles	

Change	Description	Date
AWSAuditManagerServiceRolePolicy – Update to an existing policy	We added the following permissions to `AWSAuditManagerServiceRolePolicy` . AWS Audit Manager can now perform the following actions to collect automated evidence about the resources in your AWS account. • `iam:ListAttachedGroupPolicies` • `iam:ListAttachedUserPolicies` • `iam:ListGroupsForUser` • `es:ListDomainNames` We also added a new resource in the `APIGatewayAccess` section of the policy (`arn:aws:apigateway:*::/restapis`). The policy now grants the specified permission (in this case, the `apigateway:GET` action) not only on the stages and stage resources of API Gateway REST APIs, but also on the REST APIs themselves. This change effectively expands the scope of the policy to include the ability to retrieve information about the API Gateway REST APIs themselves, in addition to the stages and stage resources associated with those APIs.	05/17/2024

Change	Description	Date
AWSAuditManagerAdministratorAccess – Update to an existing policy	We added the following permissions to `AWSAuditManagerAdministratorAccess` : • `controlcatalog:ListCommonControls` • `controlcatalog:ListDomains` • `controlcatalog:ListObjectives` This update allows you to view the control domains, control objectives, and common controls that are provided by AWS Control Catalog. These permissions are required if you want to use the common controls feature in AWS Audit Manager.	05/15/2024

Change	Description	Date
AWSAuditManagerServiceRolePolicy – Update to an existing policy	We added the following permissions to `AWSAuditManagerServiceRolePolicy` . AWS Audit Manager can now perform the following actions to collect automated evidence about the resources in your AWS account. • `apigateway:GET` • `autoscaling:DescribeAutoScalingGroups` • `backup:ListBackupPlans` • `cloudfront:GetDistribution` • `cloudfront:GetDistributionConfig` • `cloudfront:ListDistributions` • `cloudtrail:GetTrail` • `cloudtrail:ListTrails` • `dynamodb:DescribeContinuousBackups` • `dynamodb:DescribeBackup` • `dynamodb:DescribeTableReplicaAutoScaling` • `ec2:DescribeInstanceCreditSpecifications` • `ec2:DescribeInstanceAttribute` • `ec2:DescribeSecurityGroupRules` • `ec2:DescribeVpcEndpointConnections` • `ec2:DescribeVpcEndpointServiceConfigurations` • `ec2:GetLaunchTemplateData`	05/15/2024

Change	Description	Date
	• es:DescribeDomains • es:DescribeDomain • es:DescribeDomainConfig • iam:GetAccessKeyLastUsed • iam:GetGroupPolicy • iam:GetPolicy • iam:GetPolicyVersion • iam:GetRolePolicy • iam:GetUser • iam:GetUserPolicy • iam:ListAccessKeys • iam:ListAttachedRolePolicies • iam:ListMfaDeviceTags • iam:ListMfaDevices • iam:ListPolicyVersions • logs:GetDataProtectionPolicy • rds:DescribeDBInstanceAutomatedBackups • rds:DescribeDBClusterEndpoints • rds:DescribeDBClusterParameterGroups • redshift:DescribeClusterSnapshots • redshift:DescribeLoggingStatus • s3:GetBucketAcl • s3:GetBucketLogging • s3:GetBucketOwnershipControls • s3:GetBucketTagging	

Change	Description	Date
	• sagemaker:DescribeEndpointConfig • sagemaker:ListEndpointConfigs • secretsmanager:DescribeSecret • secretsmanager:ListSecrets • sns:ListTagsForResource • waf-regional:GetRule • waf-regional:GetWebAcl • waf-regional:ListRules • waf:GetRule • waf:GetRuleGroup • waf:ListRuleGroups • waf:ListRules • waf:ListWebAcls • wafv2:ListWebAcls	
AWSAuditManagerServiceRolePolicy – Update to an existing policy	The service-linked role now allows AWS Audit Manager to perform the s3:GetBucketPolicy action. This API action is required to support the AWS Generative AI Best Practices Framework v2. It allows Audit Manager to collect automated evidence about the policy restrictions that are in place for your generative AI model data training data sets. The GetBucketPolicy action operates within the scope of the AWS account where the service-linked-role is available. It can't access cross-account bucket policies.	12/06/2023

Change	Description	Date
AWSAuditManagerServiceRolePolicy – Update to an existing policy	We added the following permissions to `AWSAuditManagerServiceRolePolicy` . AWS Audit Manager can now perform the following actions to collect automated evidence about the resources in your AWS account. • `acm:GetAccountConfiguration` • `acm:ListCertificates` • `backup:ListRecoveryPointsByResource` • `bedrock:GetCustomModel` • `bedrock:GetFoundationModel` • `bedrock:GetModelCustomizationJob` • `bedrock:GetModelInvocationLoggingConfiguration` • `bedrock:ListCustomModels` • `bedrock:ListFoundationModels` • `bedrock:ListModelCustomizationJobs` • `cloudtrail:LookupEvents` • `cloudwatch:DescribeAlarmsForMetric` • `cloudwatch:GetMetricStatistics` • `cloudwatch:ListMetrics` • `directconnect:DescribeDirectConnectGateways` • `directconnect:DescribeVirtualGateways` • `dynamodb:ListBackups`	11/06/2023

Change	Description	Date
	• dynamodb:ListGlobalTables • ec2:DescribeAddresses • ec2:DescribeCustomerGateways • ec2:DescribeEgressOnlyInternetGateways • ec2:DescribeInternetGateways • ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations • ec2:DescribeLocalGateways • ec2:DescribeLocalGatewayVirtualInterfaces • ec2:DescribeNatGateways • ec2:DescribeTransitGateways • ec2:DescribeVpcPeeringConnections • ec2:DescribeVpnConnections • ec2:DescribeVpnGateways • ec2:GetEbsDefaultKmsKeyId • ec2:GetEbsEncryptionByDefault • ecs:DescribeClusters • eks:DescribeAddonVersions • elasticache:DescribeCacheClusters • elasticache:DescribeServiceUpdates • elasticfilesystem:DescribeAccessPoints • elasticloadbalancing:DescribeLoadBalancers	

Change	Description	Date
	• elasticloadbalancing:DescribeSslPolicies • elasticloadbalancing:DescribeTargetGroups • elasticmapreduce:ListClusters • elasticmapreduce:ListSecurityConfigurations • events:ListConnections • events:ListEventBuses • events:ListEventSources • events:ListRules • firehose:ListDeliveryStreams • fsx:DescribeFileSystems • iam:GetAccountPasswordPolicy • iam:GetCredentialReport • iam:ListOpenIdConnectProviders • iam:ListSamlProviders • iam:ListVirtualMFADevices • kafka:ListClusters • kafka:ListKafkaVersions • kinesis:ListStreams • lambda:ListFunctions • logs:DescribeDestinations • logs:DescribeExportTasks • logs:DescribeLogGroups • logs:DescribeMetricFilters • logs:DescribeResourcePolicies • logs:FilterLogEvents • rds:DescribeCertificates	

Change	Description	Date
	• rds:DescribeDbClusterEndpoints • rds:DescribeDbClusterParameterGroups • rds:DescribeDbClusters • rds:DescribeDbSecurityGroups • redshift:DescribeClusters • s3:GetBucketPublicAccessBlock • s3:GetBucketVersioning • sns:ListTopics • sqs:ListQueues • waf-regional:GetLoggingConfiguration • waf-regional:ListRuleGroups • waf-regional:ListSubscribedRuleGroups • waf-regional:ListWebACLs	
AWSAuditManagerServiceRolePolicy – Update to an existing policy	We added the following permissions to AWSAuditManagerServiceRolePolicy : • dynamodb:DescribeTable • dynamodb:ListTables • ec2:DescribeVolumes • kms:GetKeyPolicy • kms:GetKeyRotationStatus • kms:ListKeyPolicies • rds:DescribeDBInstances • redshift:DescribeClusters • s3:GetEncryptionConfiguration • s3:ListAllMyBuckets	07/07/2022

Change	Description	Date
AWSAuditManagerServiceRolePolicy – Update to an existing policy	The service-linked role now allows AWS Audit Manager to perform the `organizations:DescribeOrganization` action. We also scoped down the `CreateEventsAccess` resource from a wildcard (*) to a specific type of resource (`arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver`). Lastly, we added a `Null` condition operator for the `events:source` condition key to confirm that a source value exists and its value is not null.	05/20/2022
AWSAuditManagerAdministratorAccess – Update to an existing policy	We updated the key condition policy for `events:source` to reflect that this is a multi-valued key.	04/29/2022
AWSAuditManagerServiceRolePolicy – Update to an existing policy	We updated the key condition policy for `events:source` to reflect that this is a multi-valued key.	03/16/2022
AWS Audit Manager started tracking changes	AWS Audit Manager started tracking changes for its AWS managed policies.	05/06/2021

Troubleshooting AWS Audit Manager identity and access

Use the following information to help you diagnose and fix common issues that you might encounter when working with Audit Manager and IAM.

Topics

- I am not authorized to perform an action in AWS Audit Manager
- I am not authorized to perform iam:PassRole
- I want to allow people outside of my AWS account to access my AWS Audit Manager resources

I am not authorized to perform an action in AWS Audit Manager

The `AccessDeniedException` error appears when a user doesn't have permission to use AWS Audit Manager or the Audit Manager API operations.

In this case, your administrator must update the policy to allow you access.

I am not authorized to perform iam:PassRole

If you receive an error that you're not authorized to perform the `iam:PassRole` action, your policies must be updated to allow you to pass a role to Audit Manager.

Some AWS services allow you to pass an existing role to that service instead of creating a new service role or service-linked role. To do this, you must have permissions to pass the role to the service.

The following example error occurs when an IAM user named `marymajor` tries to use the console to perform an action in Audit Manager. However, the action requires the service to have permissions that are granted by a service role. Mary does not have permissions to pass the role to the service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In this case, Mary's policies must be updated to allow her to perform the `iam:PassRole` action.

If you need help, contact your AWS administrator. Your administrator is the person who provided you with your sign-in credentials.

I want to allow people outside of my AWS account to access my AWS Audit Manager resources

You can create a role that users in other accounts or people outside of your organization can use to access your resources. You can specify who is trusted to assume the role. For services that support resource-based policies or access control lists (ACLs), you can use those policies to grant people access to your resources.

To learn more, consult the following:

- To learn whether Audit Manager supports these features, see How AWS Audit Manager works with IAM.

- To learn how to provide access to your resources across AWS accounts that you own, see Providing access to an IAM user in another AWS account that you own in the *IAM User Guide*.
- To learn how to provide access to your resources to third-party AWS accounts, see Providing access to AWS accounts owned by third parties in the *IAM User Guide*.
- To learn how to provide access through identity federation, see Providing access to externally authenticated users (identity federation) in the *IAM User Guide*.
- To learn the difference between using roles and resource-based policies for cross-account access, see Cross account resource access in IAM in the *IAM User Guide*.

Using service-linked roles for AWS Audit Manager

AWS Audit Manager 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 Audit Manager. Service-linked roles are predefined by Audit Manager 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 Audit Manager easier because you don't have to manually add the necessary permissions. Audit Manager defines the permissions of its service-linked roles, and unless defined otherwise, only Audit Manager 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 Audit Manager

Audit Manager uses the service-linked role named **`AWSServiceRoleForAuditManager`**, which enables access to AWS services and resources used or managed by AWS Audit Manager.

The `AWSServiceRoleForAuditManager` service-linked role trusts the `auditmanager.amazonaws.com` service to assume the role.

The role permissions policy, `AWSAuditManagerServiceRolePolicy`, allows Audit Manager to collect automated evidence about your AWS usage. More specifically, it can take the following actions on your behalf.

- Audit Manager can use AWS Security Hub to collect **compliance check** evidence. In this case, Audit Manager uses the following permission to report the results of security checks directly from AWS Security Hub. It then attaches the results to your relevant assessment controls as evidence.
  - `securityhub:DescribeStandards`

  > **Note**
  >
  > For more information about which specific Security Hub controls Audit Manager can describe, see AWS Security Hub controls supported by AWS Audit Manager.

- Audit Manager can use AWS Config to collect **compliance check** evidence. In this case, Audit Manager uses the following permissions to report the results of AWS Config rule evaluations directly from AWS Config. It then attaches the results to your relevant assessment controls as evidence.
  - `config:DescribeConfigRules`
  - `config:DescribeDeliveryChannels`
  - `config:ListDiscoveredResources`

  > **Note**
  >
  > For more information about which specific AWS Config rules Audit Manager can describe, see AWS Config Rules supported by AWS Audit Manager.

- Audit Manager can use AWS CloudTrail to collect **user activity** evidence. In this case, Audit Manager uses the following permissions to capture user activity from CloudTrail logs. It then attaches the activity to your relevant assessment controls as evidence.
  - `cloudtrail:DescribeTrails`
  - `cloudtrail:LookupEvents`

  > **Note**
  >
  > For more information about which specific CloudTrail events Audit Manager can describe, see AWS CloudTrail event names supported by AWS Audit Manager.

- Audit Manager can use AWS API calls to collect **resource configuration** evidence. In this case, Audit Manager uses the following permissions to call read-only APIs that describe your resource

configurations for the following AWS services. It then attaches the API responses to your relevant assessment controls as evidence.

- acm:GetAccountConfiguration
- acm:ListCertificates
- apigateway:GET
- autoscaling:DescribeAutoScalingGroups
- backup:ListBackupPlans
- backup:ListRecoveryPointsByResource
- bedrock:GetCustomModel
- bedrock:GetFoundationModel
- bedrock:GetModelCustomizationJob
- bedrock:GetModelInvocationLoggingConfiguration
- bedrock:ListCustomModels
- bedrock:ListFoundationModels
- bedrock:ListGuardrails
- bedrock:ListModelCustomizationJobs
- cloudfront:GetDistribution
- cloudfront:GetDistributionConfig
- cloudfront:ListDistributions
- cloudtrail:DescribeTrails
- cloudtrail:GetTrail
- cloudtrail:ListTrails
- cloudtrail:LookupEvents
- cloudwatch:DescribeAlarms
- cloudwatch:DescribeAlarmsForMetric
- cloudwatch:GetMetricStatistics
- cloudwatch:ListMetrics
- cognito-idp:DescribeUserPool
- config:DescribeConfigRules
- config:DescribeDeliveryChannels

- config:ListDiscoveredResources
- directconnect:DescribeDirectConnectGateways
- directconnect:DescribeVirtualGateways
- dynamodb:DescribeBackup
- dynamodb:DescribeContinuousBackups
- dynamodb:DescribeTable
- dynamodb:DescribeTableReplicaAutoScaling
- dynamodb:ListBackups
- dynamodb:ListGlobalTables
- dynamodb:ListTables
- ec2:DescribeAddresses
- ec2:DescribeCustomerGateways
- ec2:DescribeEgressOnlyInternetGateways
- ec2:DescribeFlowLogs
- ec2:DescribeInstanceCreditSpecifications
- ec2:DescribeInstanceAttribute
- ec2:DescribeInstances
- ec2:DescribeInternetGateways
- ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations
- ec2:DescribeLocalGateways
- ec2:DescribeLocalGatewayVirtualInterfaces
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSecurityGroupRules
- ec2:DescribeSnapshots
- ec2:DescribeTransitGateways
- ec2:DescribeVolumes
- ec2:DescribeVpcEndpoints

- ec2:DescribeVpcEndpointConnections
- ec2:DescribeVpcEndpointServiceConfigurations
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DescribeVpnConnections
- ec2:DescribeVpnGateways
- ec2:GetEbsDefaultKmsKeyId
- ec2:GetEbsEncryptionByDefault
- ec2:GetLaunchTemplateData
- ecs:DescribeClusters
- eks:DescribeAddonVersions
- elasticache:DescribeCacheClusters
- elasticache:DescribeServiceUpdates
- elasticfilesystem:DescribeAccessPoints
- elasticfilesystem:DescribeFileSystems
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeSslPolicies
- elasticloadbalancing:DescribeTargetGroups
- elasticmapreduce:ListClusters
- elasticmapreduce:ListSecurityConfigurations
- es:DescribeDomains
- es:DescribeDomain
- es:DescribeDomainConfig
- es:ListDomainNames
- events:DeleteRule
- events:DescribeRule
- events:DisableRule
- events:EnableRule
- events:ListConnections
- events:ListEventBuses

- events:ListEventSources
- events:ListRules
- events:ListTargetsByRule
- events:PutRule
- events:PutTargets
- events:RemoveTargets
- firehose:ListDeliveryStreams
- fsx:DescribeFileSystems
- guardduty:ListDetectors
- iam:GenerateCredentialReport
- iam:GetAccessKeyLastUsed
- iam:GetAccountAuthorizationDetails
- iam:GetAccountPasswordPolicy
- iam:GetAccountSummary
- iam:GetCredentialReport
- iam:GetGroupPolicy
- iam:GetPolicy
- iam:GetPolicyVersion
- iam:GetRolePolicy
- iam:GetUser
- iam:GetUserPolicy
- iam:ListAccessKeys
- iam:ListAttachedGroupPolicies
- iam:ListAttachedRolePolicies
- iam:ListAttachedUserPolicies
- iam:ListEntitiesForPolicy
- iam:ListGroupPolicies
- iam:ListGroups
- iam:ListGroupsForUser
- iam:ListMfaDeviceTags

- iam:ListMfaDevices
- iam:ListOpenIdConnectProviders
- iam:ListPolicies
- iam:ListPolicyVersions
- iam:ListRolePolicies
- iam:ListRoles
- iam:ListSamlProviders
- iam:ListUserPolicies
- iam:ListUsers
- iam:ListVirtualMFADevices
- kafka:ListClusters
- kafka:ListKafkaVersions
- kinesis:ListStreams
- kms:DescribeKey
- kms:GetKeyPolicy
- kms:GetKeyRotationStatus
- kms:ListGrants
- kms:ListKeyPolicies
- kms:ListKeys
- lambda:ListFunctions
- license-manager:ListAssociationsForLicenseConfiguration
- license-manager:ListLicenseConfigurations
- license-manager:ListUsageForLicenseConfiguration
- logs:DescribeDestinations
- logs:DescribeExportTasks
- logs:DescribeLogGroups
- logs:DescribeMetricFilters
- logs:DescribeResourcePolicies
- logs:FilterLogEvents
- logs:GetDataProtectionPolicy

- organizations:DescribeOrganization
- organizations:DescribePolicy
- rds:DescribeCertificates
- rds:DescribeDBClusterEndpoints
- rds:DescribeDBClusterParameterGroups
- rds:DescribeDBClusters
- rds:DescribeDBInstances
- rds:DescribeDBInstanceAutomatedBackups
- rds:DescribeDBSecurityGroups
- redshift:DescribeClusters
- redshift:DescribeClusterSnapshots
- redshift:DescribeLoggingStatus
- route53:GetQueryLoggingConfig
- s3:GetBucketAcl
- s3:GetBucketLogging
- s3:GetBucketOwnershipControls
- s3:GetBucketPolicy
  - This API action operates within the scope of the AWS account where the service-linked-role is available. It can't access cross-account bucket policies.
- s3:GetBucketPublicAccessBlock
- s3:GetBucketTagging
- s3:GetBucketVersioning
- s3:GetEncryptionConfiguration
- s3:GetLifecycleConfiguration
- s3:ListAllMyBuckets
- sagemaker:DescribeAlgorithm
- sagemaker:DescribeDomain
- sagemaker:DescribeEndpoint
- sagemaker:DescribeEndpointConfig
- sagemaker:DescribeFlowDefinition

- sagemaker:DescribeHumanTaskUi
- sagemaker:DescribeLabelingJob
- sagemaker:DescribeModel
- sagemaker:DescribeModelBiasJobDefinition
- sagemaker:DescribeModelCard
- sagemaker:DescribeModelQualityJobDefinition
- sagemaker:DescribeTrainingJob
- sagemaker:DescribeUserProfile
- sagemaker:ListAlgorithms
- sagemaker:ListDomains
- sagemaker:ListEndpointConfigs
- sagemaker:ListEndpoints
- sagemaker:ListFlowDefinitions
- sagemaker:ListHumanTaskUis
- sagemaker:ListLabelingJobs
- sagemaker:ListModels
- sagemaker:ListModelBiasJobDefinitions
- sagemaker:ListModelCards
- sagemaker:ListModelQualityJobDefinitions
- sagemaker:ListMonitoringAlerts
- sagemaker:ListMonitoringSchedules
- sagemaker:ListTrainingJobs
- sagemaker:ListUserProfiles
- securityhub:DescribeStandards
- secretsmanager:DescribeSecret
- secretsmanager:ListSecrets
- sns:ListTagsForResource
- sns:ListTopics
- sqs:ListQueues
- waf-regional:GetLoggingConfiguration

- `waf-regional:GetRule`
- `waf-regional:GetWebAcl`
- `waf-regional:ListRuleGroups`
- `waf-regional:ListRules`
- `waf-regional:ListSubscribedRuleGroups`
- `waf-regional:ListWebACLs`
- `waf:GetRule`
- `waf:GetRuleGroup`
- `waf:ListActivatedRulesInRuleGroup`
- `waf:ListRuleGroups`
- `waf:ListRules`
- `waf:ListWebAcls`
- `wafv2:ListWebAcls`

> **Note**
>
> For more information about the specific API calls that Audit Manager can describe, see Supported API calls for custom control data sources.

To view the full permissions details of the service-linked role `AWSServiceRoleForAuditManager`, see AWSAuditManagerServiceRolePolicy in the *AWS Managed Policy Reference Guide*.

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*.

Creating the AWS Audit Manager service-linked role

You don't need to manually create a service-linked role. When you enable AWS Audit Manager, the service automatically creates the service-linked role for you. You can enable Audit Manager from the onboarding page of the AWS Management Console, or via the API or AWS CLI. For more information, see Enabling AWS Audit Manager in this user guide.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account.

Editing the AWS Audit Manager service-linked role

AWS Audit Manager doesn't allow you to edit the `AWSServiceRoleForAuditManager` service-linked role. After you create a service-linked role, you can't 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*.

To allow an IAM entity to edit the description of the `AWSServiceRoleForAuditManager` service-linked role

Add the following statement to the permissions policy for the IAM entity that needs to edit the description of a service-linked role.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:UpdateRoleDescription"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/
AWSServiceRoleForAuditManager*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "auditmanager.amazonaws.com"}}
}
```

Deleting the AWS Audit Manager service-linked role

If you no longer need to use Audit Manager, we recommend that you delete the `AWSServiceRoleForAuditManager` service-linked role. That way, you don't have an unused entity that isn't actively monitored or maintained. However, you must clean up the service-linked role before you can delete it.

Cleaning up the service-linked role

Before you can use IAM to delete the Audit Manager service-linked role, you must first confirm that the role has no active sessions and remove any resources used by the role. To do so, ensure that Audit Manager is deregistered in all AWS Regions. After you deregister, Audit Manager no longer uses the service-linked role.

For instructions on how to deregister Audit Manager, see the following resources:

- Disabling AWS Audit Manager in this guide
- DeregisterAccount in the *AWS Audit Manager API Reference*
- deregister-account in the *AWS CLI Reference for AWS Audit Manager*

For instructions on how to delete Audit Manager resources manually, see Deletion of Audit Manager data in this guide.

Deleting the service-linked role

You can delete the service-linked role using the IAM console, the AWS Command Line Interface (AWS CLI), or the IAM API.

IAM console

Follow these steps to delete a service-linked role in the IAM console.

To delete a service-linked role (console)

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane of the IAM console, choose **Roles**. Then select the check box next to `AWSServiceRoleForAuditManager`, not the name or row itself.
3. Under **Role actions** at the top of the page, choose **Delete**.
4. In the confirmation dialog box, review the last accessed information, which shows when each of the selected roles last accessed an AWS service. This helps you to confirm whether the role is currently active. If you want to proceed, enter **`AWSServiceRoleForAuditManager`** in the text input field and choose **Delete** to submit the service-linked role for deletion.
5. Watch the IAM console notifications to monitor the progress of the service-linked role deletion. Because the IAM service-linked role deletion is asynchronous, after you submit the role for deletion, the deletion task can succeed or fail. If the task succeeds, then the role is removed from the list and a success message appears at the top of the page.

AWS CLI

You can use IAM commands from the AWS CLI to delete a service-linked role.

To delete a service-linked role (AWS CLI)

1. Enter the following command to list the role in your account:

```
aws iam get-role --role-name AWSServiceRoleForAuditManager
```

2. Because a service-linked role can't be deleted if it's being used or has associated resources, you must submit a deletion request. That request can be denied if these conditions aren't met. You must capture the `deletion-task-id` from the response to check the status of the deletion task.

   Enter the following command to submit a service-linked role deletion request:

```
aws iam delete-service-linked-role --role-name AWSServiceRoleForAuditManager
```

3. Use the following command to check the status of the deletion task:

```
aws iam get-service-linked-role-deletion-status --deletion-task-id deletion-task-id
```

   The status of the deletion task can be `NOT_STARTED`, `IN_PROGRESS`, `SUCCEEDED`, or `FAILED`. If the deletion fails, the call returns the reason that it failed so that you can troubleshoot.

IAM API

You can use the IAM API to delete a service-linked role.

To delete a service-linked role (API)

1. Call GetRole to list the role in your account. In the request, specify `AWSServiceRoleForAuditManager` as the `RoleName`.
2. Because a service-linked role can't be deleted if it's being used or has associated resources, you must submit a deletion request. That request can be denied if these conditions aren't met. You must capture the `DeletionTaskId` from the response to check the status of the deletion task.

   To submit a deletion request for a service-linked role, call DeleteServiceLinkedRole. In the request, specify `AWSServiceRoleForAuditManager` as the `RoleName`.

3. To check the status of the deletion, call GetServiceLinkedRoleDeletionStatus. In the request, specify the `DeletionTaskId`.

   The status of the deletion task can be `NOT_STARTED`, `IN_PROGRESS`, `SUCCEEDED`, or `FAILED`. If the deletion fails, the call returns the reason that it failed so that you can troubleshoot.

Tips for deleting the Audit Manager service-linked role

The deletion process for the Audit Manager service-linked role might fail if Audit Manager is using the role or has associated resources. This can happen in the following scenarios:

1. Your account is still registered with Audit Manager in one or more AWS Regions.
2. Your account is part of an AWS organization, and the management account or the delegated administrator account is still onboarded to Audit Manager.

To resolve a failed deletion issue, start by checking whether your AWS account is part of an Organization. You can do this by calling the DescribeOrganization API operation, or by navigating to the AWS Organizations console.

If your AWS account is part of an organization

1. Use your management account to remove your delegated administrator in Audit Manager in all AWS Regions where you added one.
2. Use your management account to deregister Audit Manager in all AWS Regions where you used the service.
3. Try again to delete the service-linked role by following the steps in the previous procedure.

If your AWS account is not part of an organization

1. Make sure that you deregistered Audit Manager in all AWS Regions where you used the service.
2. Try again to delete the service-linked role by following the steps in the previous procedure.

After you deregister from Audit Manager, the service will stop using the service-linked role. You can then delete the role successfully.

Supported Regions for AWS Audit Manager service-linked roles

AWS Audit Manager supports using service-linked roles in all of the AWS Regions where the service is available. For more information, see AWS service endpoints.

Compliance validation for AWS Audit Manager

To learn whether an AWS service is within the scope of specific compliance programs, see AWS services in Scope by Compliance Program and choose the compliance program that you are interested in. 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 Compliance & Governance – These solution implementation guides discuss architectural considerations and provide steps for deploying security and compliance features.
- HIPAA Eligible Services Reference – Lists HIPAA eligible services. Not all AWS services are HIPAA eligible.
- AWS Compliance Resources – This collection of workbooks and guides might apply to your industry and location.
- AWS Customer Compliance Guides – Understand the shared responsibility model through the lens of compliance. The guides summarize the best practices for securing AWS services and map the guidance to security controls across multiple frameworks (including National Institute of Standards and Technology (NIST), Payment Card Industry Security Standards Council (PCI), and International Organization for Standardization (ISO)).
- 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. Security Hub uses security controls to evaluate your AWS resources and to check your compliance against security industry standards and best practices. For a list of supported services and controls, see Security Hub controls reference.

- Amazon GuardDuty – This AWS service detects potential threats to your AWS accounts, workloads, containers, and data by monitoring your environment for suspicious and malicious activities. GuardDuty can help you address various compliance requirements, like PCI DSS, by meeting intrusion detection requirements mandated by certain compliance frameworks.
- 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.

Understanding resilience in AWS Audit Manager

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 Audit Manager

As a managed service, AWS Audit Manager is protected by AWS global network security. For information about AWS security services and how AWS protects infrastructure, see AWS Cloud Security. To design your AWS environment using the best practices for infrastructure security, see Infrastructure Protection in *Security Pillar AWS Well-Architected Framework*.

You use AWS published API calls to access AWS Audit Manager through the network. Clients must support the following:

- Transport Layer Security (TLS). We require TLS 1.2 and recommend TLS 1.3.
- Cipher suites with perfect forward secrecy (PFS) such as DHE (Ephemeral Diffie-Hellman) or ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). 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.

You can call these API operations from any network location, but AWS Audit Manager does support resource-based access policies, which can include restrictions based on the source IP address. You can also use Audit Manager policies to control access from specific Amazon Virtual Private Cloud (Amazon VPC) endpoints or specific VPCs. Effectively, this isolates network access to a given Audit Manager resource from only the specific VPC within the AWS network.

AWS Audit Manager and interface VPC endpoints (AWS PrivateLink)

You can establish a private connection between your VPC and AWS Audit Manager by creating an *interface VPC endpoint*. Interface endpoints are powered by AWS PrivateLink, a technology that enables you to privately access Audit Manager APIs without an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC don't need public IP addresses to communicate with Audit Manager APIs. Traffic between your VPC and AWS Audit Manager does not leave the AWS network.

Each interface endpoint is represented by one or more Elastic Network Interfaces in your subnets.

For more information, see Interface VPC endpoints (AWS PrivateLink) in the *Amazon VPC User Guide*.

Considerations for AWS Audit Manager VPC endpoints

Before you set up an interface VPC endpoint for AWS Audit Manager, ensure that you review Interface endpoint properties and limitations in the *Amazon VPC User Guide*.

AWS Audit Manager supports making calls to all of its API actions from your VPC.

Creating an interface VPC endpoint for AWS Audit Manager

You can create a VPC endpoint for the AWS Audit Manager service using either the Amazon VPC console or the AWS Command Line Interface (AWS CLI). For more information, see Creating an interface endpoint in the *Amazon VPC User Guide*.

Create a VPC endpoint for AWS Audit Manager using the following service name:

- `com.amazonaws.region.auditmanager`

If you enable private DNS for the endpoint, you can make API requests to AWS Audit Manager using its default DNS name for the Region, for example, `auditmanager.us-east-1.amazonaws.com`.

For more information, see Accessing a service through an interface endpoint in the *Amazon VPC User Guide*.

Creating a VPC endpoint policy for AWS Audit Manager

You can attach an endpoint policy to your VPC endpoint that controls access to AWS Audit Manager. The policy specifies the following information:

- The principal that can perform actions.
- The actions that can be performed.
- The resources on which actions can be performed.

For more information, see Controlling access to services with VPC endpoints in the *Amazon VPC User Guide*.

Example: VPC endpoint policy for AWS Audit Manager actions

The following is an example of an endpoint policy for AWS Audit Manager. When attached to an endpoint, this policy grants access to the listed Audit Manager actions for all principals on all resources.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "auditmanager:GetAssessment",
            "auditmanager:GetServicesInScope",
            "auditmanager:ListNotifications"
         ],
         "Resource":"*"
      }
   ]
}
```

Logging and monitoring in AWS Audit Manager

Monitoring is an important part of maintaining the reliability, availability, and performance of Audit Manager and your other AWS solutions. AWS provides the following monitoring tools to watch Audit Manager, report when something is wrong, and take automatic actions when appropriate:

- *AWS CloudTrail* captures API calls and related events made by or on behalf of your AWS account and delivers the log files to an Amazon S3 bucket that you specify. You can identify which users and accounts called AWS, the source IP address from which the calls were made, and when the calls occurred. For more information, see the AWS CloudTrail User Guide.
- *Amazon EventBridge* is a serverless event bus service that makes it easy to connect your applications with data from a variety of sources. EventBridge delivers a stream of real-time data from your own applications, Software-as-a-Service (SaaS) applications, and AWS services and routes that data to targets such as Lambda. This enables you to monitor events that happen in services, and build event-driven architectures. For more information, see the Amazon EventBridge User Guide.

Monitoring AWS Audit Manager with Amazon EventBridge

Amazon EventBridge helps you automate your AWS services and respond automatically to system events such as application availability issues or resource changes.

You can use EventBridge rules to detect and react to Audit Manager events. Based on the rules that you create, EventBridge invokes one or more target actions when an event matches the values that 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.

For example, you can detect whenever the following Audit Manager events occur in your account:

- An audit owner creates, updates, or deletes an assessment
- An audit owner delegates a control set for review
- A delegate completes their review and submits the reviewed control set back to the audit owner
- An audit owner updates the status of an assessment control

The actions that can be automatically triggered include the following:

- Use an AWS Lambda function to pass a notification to a Slack channel.
- Push data about the check to an Amazon Kinesis Data Streams to support comprehensive and real-time status monitoring.
- Send an Amazon Simple Notification Service (Amazon SNS) topic to your email.
- Get notified with an Amazon CloudWatch alarm action.

> **Note**
>
> Audit Manager delivers events on a *durable* basis. This means that Audit Manager will successfully attempt to deliver events to EventBridge at least once. In cases where events can't be delivered because of an EventBridge service disruption, they will be retried again later by Audit Manager for up to 24 hours.

EventBridge example format for Audit Manager

The following JSON code shows an example of an assessment creation event in Audit Manager. For information on any of the fields in this event, see Event structure reference.

```
{
    "version": "0",
    "id": "55c5a6f3-6183-3989-49ec-a3c998857644",
    "detail-type": "Assessment Created",
    "source": "aws.auditmanager",
    "account": "111122223333",
    "time": "2023-07-27T00:38:33Z",
    "region": "us-west-2",
    "resources":
        [
            "arn:aws:auditmanager:us-west-2:111122223333:assessment/a1b2c3d4-e5f6-g7h8-
i9j0-k1l2m3n4o5p6"
        ],
    "detail":
    {
        "eventID": "4e939b2f-9429-3141-beec-d640d83ef68e",
        "author": "arn:aws:sts::111122223333:assumed-role/roleName/role-session-name",
        "assessmentTenantId": "111122223333",
        "assessmentName": "myAssessment",
        "eventTime": 1690418289068,
```

```
        "eventName": "CREATE",
        "eventType": "ASSESSMENT",
        "assessmentID": "a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6"
    }
}
```

Prerequisites for creating an EventBridge rule

Before you create rules for Audit Manager events, we recommend that you do the following:

- Familiarize yourself with events, rules, and targets in EventBridge. For more information, see What is Amazon EventBridge? in the *Amazon EventBridge User Guide*.
- Create a target to use in your event rule. For example, you can create an Amazon SNS topic so that whenever a control set review is completed, you'll receive a text message or email. For more information, see EventBridge targets.

Creating an EventBridge rule for Audit Manager

Follow these steps to create an EventBridge rule that triggers on an event emitted by Audit Manager. Events are emitted on a best effort basis.

To create an EventBridge rule for Audit Manager

1. Open the Amazon EventBridge console at https://console.aws.amazon.com/events/.
2. In the navigation pane, choose **Rules**.
3. Choose **Create rule**.
4. On the **Define rule detail** page, enter a name and description for the rule.
5. Keep the default values for **Event bus** and **Rule type**, and then choose **Next**.
6. On the **Build event pattern** page, for **Event source**, choose **AWS events or EventBridge partner events**.
7. For **Creation method**, choose **Custom pattern (JSON editor)**.
8. Under **Event pattern**, write an event pattern in JSON and specify the fields that you want to use for matching.

   To match an Audit Manager event, you can use the following simple pattern:

   ```
   {
     "detail-type": ["Event"]
   ```

```
}
```

Replace *Event* with one of the following supported values:

a. Enter `Assessment Created` to get notifications when an assessment is created.

b. Enter `Assessment Updated` to get notifications when an assessment is updated.

c. Enter `Assessment Deleted` to get notifications when an assessment is deleted.

d. Enter `Assessment ControlSet Delegation Created` to get notifications when a control set is delegated for review.

e. Enter `Assessment ControlSet Reviewed` to get notifications when an assessment control set is reviewed.

f. Enter `Assessment Control Reviewed` to get notifications when an assessment control is reviewed.

> **Tip**
>
> Add more fields to your event pattern as needed. For more information about available fields, see Amazon EventBridge event patterns.

9. Choose **Next**.

10. On the **Select target(s)** page, choose the target that you created for this rule, and then configure any additional options that are required for that type. For example, if you choose Amazon SNS, make sure that your SNS topic is configured correctly so that you'll be notified by email or SMS.

> **Tip**
>
> The fields displayed vary depending on the service selected. For more information about available targets, see Targets available in the EventBridge console.

11. For many target types, EventBridge needs permissions to send events to the target. In these cases, EventBridge can create the IAM role that's needed for your rule to run.

    a. To create an IAM role automatically, choose **Create a new role for this specific resource**.

    b. To use an IAM role that you created earlier, choose **Use existing role**.

12. (Optional) Choose **Add another target** to add another target for this rule.

13. Choose **Next**.
14. (Optional) On the **Configure tags** page, add any tags and then choose **Next**.
15. On the **Review and create** page, review your rule setup and ensure that it meets your event monitoring requirements.
16. Choose **Create rule**. Your rule will now monitor for Audit Manager events and then send them to the target that you specified.

Logging AWS Audit Manager API calls with CloudTrail

Audit Manager is integrated with CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Audit Manager. CloudTrail captures all API calls for Audit Manager as events. The calls captured include calls from the Audit Manager console and code calls to the Audit Manager API operations.

If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for Audit Manager. 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 Audit Manager, 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.

Audit Manager information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When activity occurs in Audit Manager, 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 Audit Manager, 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 Audit Manager actions are logged by CloudTrail and are documented in the AWS Audit Manager API Reference. For example, calls to the `CreateControl`, `DeleteControl`, and `UpdateAssessmentFramework` API 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 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 Audit Manager 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.

The following example shows a CloudTrail log entry that demonstrates the `CreateAssessment` action.

```
{
      eventVersion:"1.05",
      userIdentity:{
        type:"IAMUser",
        principalId:"principalId",
```

```
        arn:"arn:aws:iam::accountId:user/userName",
        accountId:"111122223333",
        accessKeyId:"accessKeyId",
        userName:"userName",
        sessionContext:{
          sessionIssuer:{
          },
          webIdFederationData:{
          },
          attributes:{
            mfaAuthenticated:"false",
            creationDate:"2020-11-19T07:32:06Z"
          }
        }
      },
      eventTime:"2020-11-19T07:32:36Z",
      eventSource:"auditmanager.amazonaws.com",
      eventName:"CreateAssessment",
      awsRegion:"us-west-2",
      sourceIPAddress:"sourceIPAddress",
      userAgent:"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
      requestParameters:{
        frameworkId:"frameworkId",
        assessmentReportsDestination:{
          destination:"***",
          destinationType:"S3"
        },
        clientToken:"***",
        scope:{
          awsServices:[
            {
              serviceName:"license-manager"
            }
          ],
          awsAccounts:"***"
        },
        roles:"***",
        name:"***",
        description:"***",
        tags:"***"
      },
      responseElements:{
        assessment:"***"
```

```
    },
    requestID:"0d950f8c-5211-40db-8c37-2ed38ffcc894",
    eventID:"a782029a-959e-4549-81df-9f6596775cb0",
    readOnly:false,
    eventType:"AwsApiCall",
    recipientAccountId:"recipientAccountId"
  }
```

Understanding configuration and vulnerability analysis in AWS Audit Manager

Configuration and IT controls are a shared responsibility between AWS and you, our customer. For more information, see the AWS shared responsibility model.

Disabling AWS Audit Manager

You can disable Audit Manager if you no longer want to use the service. When you disable Audit Manager, you also have the option to delete all of your data.

By default, your data isn't deleted when you disable Audit Manager. Your evidence data is retained for two years from the time of its creation. Your other Audit Manager resources (including assessments, custom controls, and custom frameworks) are retained indefinitely, and will be available if you re-enable Audit Manager in the future. For more information about data retention, see Data Protection in this guide.

If you choose to delete your data, Audit Manager deletes all evidence data along with all of the Audit Manager resources that you created (including assessments, custom controls, and custom frameworks). All of your data is deleted within seven days of disabling Audit Manager.

Topics

Procedure

You can disable Audit Manager using the Audit Manager console, the AWS Command Line Interface (AWS CLI), or the Audit Manager API.

Warning

- When you disable Audit Manager, your access is revoked and the service no longer collects evidence for any existing assessments. You can't access anything in the service unless you re-enable Audit Manager.
- Deleting all data is a permanent action. If you decide to re-enable Audit Manager in the future, your data won't be recoverable.

Audit Manager console

To disable Audit Manager on the Audit Manager console

1. From the **General** settings tab, go to the **Disable AWS Audit Manager** section.
2. Choose **Disable**.
3. In the pop-up window, review your current data retention setting.
    a. To proceed with your current selection, choose **Disable Audit Manager**.
    b. To change your current selection, perform the following steps:
        i. Choose **Cancel** to return to the settings page.
        ii. To use the default data retention setting, turn off **Delete all data**. This selection retains evidence data for two years from the time of its creation, and retains other Audit Manager resources indefinitely.
        iii. To delete your data, turn on **Delete all data**.
        iv. Choose **Disable**, and then choose **Disable Audit Manager** to confirm your choice.

AWS CLI

Before you start

Before you disable Audit Manager, you can run the update-settings command to set your preferred data retention policy. By default, Audit Manager retains your data. If you want to request the deletion of your data, use the `--deregistration-policy` parameter with the `deleteResources` value set to `ALL`.

```
aws auditmanager update-settings --deregistration-policy deleteResources=ALL
```

To disable Audit Manager in the AWS CLI

When you're ready to disable Audit Manager, run the deregister-account command.

```
aws auditmanager deregister-account
```

Audit Manager API

Before you start

Before you disable Audit Manager, you can use the UpdateSettings API operation to set your preferred data retention policy. By default, Audit Manager retains your data. If you want to delete your data, you can use the DeregistrationPolicy attribute to request the deletion of your data.

To disable Audit Manager using the API

When you're ready to disable Audit Manager, call the DeregisterAccount operation.

For more information, choose the previous links to read more in the *Audit Manager API Reference*. This includes information about how to use these operations and parameters in one of the language-specific AWS SDKs.

Next steps

If you need to re-enable Audit Manager after you disable it, follow these steps to get the service up and running again.

To re-enable Audit Manager after you disable it

Go to the Audit Manager service homepage and follow the steps to set up Audit Manager as a new user. For more information, see Setting up AWS Audit Manager with the recommended settings.

Tip

- If you chose to delete your data when you disabled Audit Manager, you must wait until your data is deleted before you can re-enable the service. Depending on how much data you have, this can take up to seven days. However, feel free to try re-enabling Audit Manager before then. In many cases, data is deleted in as little as one hour.
- If you chose not to delete your data when you disabled Audit Manager, your existing assessments moved into a dormant state and stopped collecting evidence as a result. To start collecting evidence again for a pre-existing assessment, edit the assessment and choose **Save** without making any changes.

Additional resources

- For more information about data retention in Audit Manager, see Data Protection in this guide.

Document history for AWS Audit Manager User Guide

The following table describes the important changes in each release of the AWS Audit Manager User Guide from December 8, 2020, onward.

Change	Description	Date
Updates to five supported frameworks	The following frameworks have been updated: • CCCS Medium Cloud Control • ISO/IEC 27001:2013 Annex A • PCI DSS V3.2.1 • PCI DSS V4.0 • SSAE-18 SOC 2	July 17, 2025
Updates to five supported frameworks	The following frameworks have been updated: • Amazon Web Services (AWS) Well Architected Framework (WAF) v10 • FedRAMP Security Baseline Controls r4 • NIST SP 800-171 Rev 2 • NIST-CSF-v1.1 • NIST-SP-800-53-r5	June 19, 2025
Updates to three supported frameworks	The following frameworks have been updated: • ACSC Essential Eight • ACSC ISM	June 4, 2025

	• CIS Critical Security Controls version 8.0, IG1	
Updated supported framework: CIS Controls v7.1, IG1	The CIS Controls v7.1, IG1 framework has been updated. For more information, see CIS Controls v7.1, IG1.	May 14, 2025
Updated s3_ListBuckets policy	AWS Audit Manager has updated the `s3_ListBuckets` policy and the documentation for `s3_GetBucketEncryption` to match the policy. For more information, see Supported API calls for custom control data sources.	March 24, 2025
Updated AWS managed policy	AWS Audit Manager has updated the AWSAuditManagerServiceRolePolicy. For more information, see AWS managed policies for AWS Audit Manager.	September 24, 2024
New supported framework : AWS generative AI best practices v2	A new prebuilt framework is now available in AWS Audit Manager. For more information, see AWS generative AI best practices framework v2.	June 11, 2024
Updated AWS managed policy	AWS Audit Manager has updated the AWSAuditManagerServiceRolePolicy. For more information, see AWS managed policies for AWS Audit Manager.	June 10, 2024

Use common controls to simplify how you run assessments against your enterprise controls	When you create a custom control, you can now use common controls as an evidence source. Each common control maps to a managed grouping of relevant AWS data sources. These predefined groupings streamline evidence collectio n by eliminating the need to identify which AWS resources need to be assessed for a given control. For information about how to find common controls and use them as evidence sources, see Control library.	June 6, 2024
Updated AWS managed policy	AWS Audit Manager has updated the AWSAuditM anagerServiceRolePolicy. For more information, see AWS managed policies for AWS Audit Manager.	May 17, 2024
Updated AWS managed policy	AWS Audit Manager has updated the AWSAuditM anagerAdministratorAccess policy. For more information, see AWS managed policies for AWS Audit Manager.	May 15, 2024

Updated AWS managed policy	AWS Audit Manager has updated the AWSAuditManagerServiceRolePolicy. For more information, see AWS managed policies for AWS Audit Manager.	May 15, 2024
Support for additional AWS API calls	You can now use additional AWS API calls as data sources for your custom controls in Audit Manager. For more information, see Supported API calls for custom control data sources.	May 15, 2024
New supported framework: PCI DSS V4.0	A new prebuilt framework is now available in AWS Audit Manager. For more informati on, see PCI DSS V4.0.	December 19, 2023
Support for additional AWS API calls	You can now use additional AWS API calls as data sources for your custom controls in Audit Manager. For more information, see Supported API calls for custom control data sources.	December 7, 2023
Updated AWS managed policy	AWS Audit Manager has updated the AWSAuditManagerServiceRolePolicy. For more information, see AWS managed policies for AWS Audit Manager.	December 6, 2023

Support for AWS Security Hub consolidated control findings	Audit Manager now supports consolidated controls in AWS Security Hub. For more information, see AWS Security Hub controls supported by AWS Audit Manager.	November 16, 2023
Integration with MetricStream	You can now ingest evidence from Audit Manager into MetricStream. For more information, see Integrations with third-party GRC products.	November 14, 2023
New supported framework : AWS generative AI best practices	A new prebuilt framework is now available in AWS Audit Manager. For more information, see AWS generative AI best practices framework v1.	November 8, 2023
Updated AWS managed policy	AWS Audit Manager has updated the AWSAuditManagerServiceRolePolicy. For more information, see AWS managed policies for AWS Audit Manager.	November 6, 2023
Integration with Amazon EventBridge	You can now monitor events that happen in AWS Audit Manager and use these events as part of your event-driven architecture. For more information, see Monitoring AWS Audit Manager with Amazon EventBridge.	August 18, 2023

Support for risk assessments and new manual evidence options	You can now use the custom control creation workflow to support risk assessments. A control can now represent a risk assessment question, and you can provide an answer by uploading a file or entering text as manual evidence. For more information, see Create a custom control and Add manual evidence.	June 12, 2023
Support for CSV exports	You can now export your evidence finder search results in CSV format. For more information, see Export your search results.	June 9, 2023
New supported framework: Australian Cyber Security Centre (ACSC) Information Security Manual	A new prebuilt framework is now available in AWS Audit Manager. For more information, see Australian Cyber Security Centre (ACSC) Information Security Manual.	March 24, 2023
Improved assessment reports	We made improvements to the format and contents of Audit Manager assessment reports. For more information about how to navigate and understand assessment reports, see Assessment reports.	March 23, 2023

Support for paginated API calls	AWS Audit Manager now supports paginated API calls as a data source for evidence collection. For more informati on, see Paginated API calls.	March 8, 2023
New supported framework: HIPAA Final Omnibus Security Rule 2013	A new prebuilt framework is now available in AWS Audit Manager. For more information, see HIPAA Final Omnibus Security Rule 2013. For differentiation purposes, the previously existing HIPAA framework (formerly named *HIPAA* in the framework library) is now named HIPAA Security Rule 2003.	March 8, 2023
Support for additional AWS API calls	You can now use an additiona l nine AWS API calls as a data source for your custom controls in Audit Manager. For more information, see Supported API calls for custom control data sources.	March 3, 2023
Updated guide to align with the IAM best practices	Updated guide to align with the IAM best practices . For more information, see Security best practices in IAM.	January 6, 2023

New data retention setting	You can now specify if you want to delete all of your data when you disable Audit Manager. For more informati on, see Disable AWS Audit Manager and Deletion of Audit Manager data.	January 6, 2023
Support for evidence finder	You can now use evidence finder to perform search queries on your evidence data. For more information, see Evidence finder.	November 18, 2022
New supported framework : Australian Cyber Security Centre (ACSC) Essential Eight	A new prebuilt framework is now available in AWS Audit Manager. For more information, see Australian Cyber Security Centre (ACSC) Essential Eight.	August 24, 2022
Updated AWS managed policy	AWS Audit Manager has updated the AWSAuditM anagerServiceRolePolicy. For more information, see AWS managed policies for AWS Audit Manager.	July 7, 2022
Updated AWS managed policy	AWS Audit Manager has updated the AWSAuditM anagerServiceRolePolicy. For more information, see AWS managed policies for AWS Audit Manager.	May 20, 2022

New supported framework : Canadian Centre for Cyber Security Medium Cloud Control Profile	A new prebuilt framework is now available in AWS Audit Manager. For more informati on, see Canadian Centre for Cyber Security Medium Cloud Control Profile.	May 6, 2022
Updated AWS managed policy	AWS Audit Manager has updated the AWSAuditM anagerAdministratorAccess policy. For more information, see AWS managed policies for AWS Audit Manager.	April 29, 2022
Support for additional AWS Config managed rules	You can now use an additiona l 91 AWS Config managed rules as a data source for your custom controls in Audit Manager. For more informati on, see Using AWS Config managed rules with AWS Audit Manager.	April 27, 2022
Support for AWS Config custom rules	You can now use AWS Config custom rules as a data source for your custom controls in Audit Manager. For more information, see Using AWS Config custom rules with AWS Audit Manager.	April 27, 2022
New supported framework: ISO/IEC 27001:2013 Annex A	A new prebuilt framework is now available in AWS Audit Manager. For more informati on, see ISO/IEC 27001:2013 Annex A.	April 7, 2022

Updated AWS managed policy	AWS Audit Manager has updated the AWSAuditManagerServiceRolePolicy. For more information, see AWS managed policies for AWS Audit Manager.	March 16, 2022
New supported frameworks: CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.4	Two new prebuilt frameworks are now available in AWS Audit Manager: *CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.4, Level 1*, and *CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.4, Level 1 and 2*. For more information, see CIS Benchmark for CIS AWS Audit Manager Foundations Benchmark v1.4.0.	March 2, 2022
New supported framework: CIS Controls v8 IG1	A new prebuilt framework is now available in AWS Audit Manager. For more information, see CIS Controls v8 IG1.	March 2, 2022
AWS Audit Manager dashboard	You can now use the Audit Manager dashboard to monitor your active assessments and quickly identify non-compliant evidence. For more information, see Using the Audit Manager dashboard.	November 18, 2021

Custom framework sharing	You can now share your custom Audit Manager frameworks with another AWS account, or replicate them into another AWS Region under your own account. For more informati on, see Sharing a custom framework.	October 22, 2021
New examples of AWS Audit Manager controls	You can now review examples of controls and learn how Audit Manager helps bring your AWS environment in line with their requireme nts. For more information, see Examples of AWS Audit Manager controls.	September 21, 2021
New supported framework : Gramm-Leach-Bliley Act (GLBA)	A new prebuilt framework is now available in AWS Audit Manager. For more informati on, see Gramm-Leach-Bliley Act (GLBA).	September 2, 2021
New troubleshooting chapter	A new troubleshooting chapter is now available. For more information, see Troubleshooting in AWS Audit Manager.	August 23, 2021

New delegation chapter and tutorial	We expanded our delegation documentation into a new chapter. For more information, see Delegations in AWS Audit Manager. We also added a new tutorial aimed at delegates who are reviewing a control set for the first time in AWS Audit Manager. For more information, see Tutorial for Delegates: Reviewing a control set.	June 25, 2021
New supported framework: NIST SP 800-171 Rev. 2	A new prebuilt framework is now available in AWS Audit Manager. For more information, see NIST SP 800-171 Rev. 2.	June 17, 2021
Improved assessment reports	We made improvements to the format and contents of AWS Audit Manager assessment reports. For more information about how to navigate and understand the new assessment reports, see Assessment reports.	June 8, 2021
New AWS managed policies page	AWS Audit Manager has started tracking changes for its managed policies. For more information, see AWS managed policies for AWS Audit Manager.	May 6, 2021

New supported framework : NIST Cybersecurity Framework version 1.1	A new prebuilt framework is now available in AWS Audit Manager. For more informati on, see NIST Cybersecurity Framework version 1.1.	May 5, 2021
New supported framework: AWS Well-Architected	A new prebuilt framework is now available in AWS Audit Manager. For more informati on, see AWS Well-Architected.	May 5, 2021
New supported framework: AWS Foundational Security Best Practices	A new prebuilt framework is now available in AWS Audit Manager. For more informati on, see AWS Foundational Security Best Practices.	May 5, 2021
New supported framework: GxP EU Annex 11	A new prebuilt framework is now available in AWS Audit Manager. For more informati on, see GxP EU Annex 11.	April 28, 2021
New supported framework : NIST 800-53 (Rev. 5) Low-Moderate-High	A new prebuilt framework is now available in AWS Audit Manager. For more informati on, see NIST 800-53 (Rev. 5) Low-Moderate-High.	March 25, 2021

New supported frameworks: CIS Benchmark for CIS AWS Audit Manager Foundations Benchmark v1.3	Two new prebuilt frameworks are now available in AWS Audit Manager: *CIS Benchmark for CIS AWS Audit Manager Foundations Benchmark v1.3.0, Level 1*, and *CIS Benchmark for CIS AWS Audit Manager Foundations Benchmark v1.3.0, Level 1 and 2*. For more information, see CIS Benchmark for CIS AWS Audit Manager Foundations Benchmark v1.3.0.	March 22, 2021
Initial release	Initial release of the AWS Audit Manager User Guide and API Reference.	December 8, 2020