Cohasset Associates

SEC 17a-4(f), FINRA 4511(c), and CFTC 1.31(c)-(d)
Compliance Assessment

Amazon Web Services (AWS) Backup

Abstract

Amazon Web Services (AWS) is a secure cloud services platform hosted by Amazon to provide modular cloud-based products and services. Amazon AWS Backup (AWS Backup) is an AWS service that provides a fully-managed data protection service for AWS products and services.

In this Report, Cohasset Associates, Inc. (Cohasset) assesses the functionality of AWS Backup (see Section 1.3, *AWS Backup Overview and Assessment Scope)* relative to the recording, storage, and retention requirements for electronic records specified by:

- Securities and Exchange Commission (SEC) Rule 17 CFR § 240.17a-4(f), which regulates exchange members, brokers or dealers.
- Financial Industry Regulatory Authority (FINRA) Rule 4511(c), which defers to the format and media requirements of SEC Rule 17a-4(f).
- Commodity Futures Trading Commission (CFTC) Rule 17 CFR § 1.31(c)-(d), which regulates commodity futures trading.

It is Cohasset's opinion that AWS Backup, when properly configured and when *Vault Lock* mode is set to *Compliance*, retains Recovery Points, containing required records, in non-rewriteable and non-erasable format and meets the relevant storage requirements set forth in the above Rules. Each record is protected from being modified, overwritten or deleted until the applied retention period is expired and any associated legal hold is released.

BENEFIT FROM COHASSET'S INDUSTRY INSIGHT AND EXPERIENCE

Core to Cohasset's practice is its delivery of records management and information governance professional consulting services, education and training. Cohasset's expert consulting services are tailored to support a multitude of regulated organizations, including those in the financial services industry. Cohasset serves both domestic and multi-national clients, aligning information lifecycle controls with their organizations' business priorities and facilitating regulatory compliance and risk mitigation, all the while generating measurable business efficiencies.

Cohasset has assessed the spectrum of storage technologies and systems designed to meet the requirements of the Securities and Exchange Commission Rule 17a-4(f), as defined by 1) the No Action Letter in 1993 (allowing broker dealers to use non-rewriteable, non-erasable digital storage media); 2) the issuance of the Rule in 1997; and 3) the Interpretive Release in 2003, which authorizes the use of erasable storage, conditioned on integrated control codes, to prevent premature deletion of records.

Table of Contents

Abstract 1

Table of Contents 2

1 | Introduction 3

- 1.1 Overview of the Regulatory Requirements 3
- 1.2 Purpose and Approach 4
- 1.3 AWS Backup Overview and Assessment Scope 5

2 | Assessment of Compliance with SEC Rule 17a-4(f) 7

- 2.1 Non-Rewriteable, Non-Erasable Record Format 7
- 2.2 Accurate Recording Process 13
- 2.3 Serialize the Original and Duplicate Units of Storage Media 14
- 2.4 Capacity to Download Indexes and Records 15
- 2.5 Duplicate Copy of the Records Stored Separately 15

3 | Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d) 17

4 | Conclusions 21

5 | Overview of Relevant Regulatory Requirements 22

- 5.1 Overview of SEC Rule 17a-4(f) Electronic Records Storage Requirements 22
- 5.2 Overview of FINRA Rule 4511(c) Electronic Records Storage Requirements 25
- 5.3 Overview of CFTC Rule 1.31(c)-(d) Electronic Regulatory Records Requirements 25

About Cohasset Associates, Inc. 27

1 | Introduction

Regulators, worldwide, establish explicit requirements for regulated entities that elect to retain books and records[1] on electronic storage media. Given the prevalence of electronic books and records, these requirements apply to most broker-dealer and commodity futures trading firms and other organizations with similarly regulated operations.

This Introduction *briefly summarizes the regulatory environment pertaining to this assessment, explains the purpose and approach for Cohasset's assessment, and provides an overview of Amazon Web Services (AWS) Backup and the scope of this assessment.*

1.1 Overview of the Regulatory Requirements

1.1.1 SEC Rule 17a-4(f) Requirements

In 17 CFR §§ 240.17a-3 and 240.17a-4, the SEC stipulates recordkeeping requirements, including retention periods, for the securities broker-dealer industry. On February 12, 1997, the SEC adopted amendments to 17 CFR § 240.17a-4 (the Rule or Rule 17a-4). These amendments to paragraph (f) expressly allow books and records to be retained on electronic storage media, subject to explicit standards.

> *The Commission is adopting a rule today which, instead of specifying the type of storage technology that may be used, sets forth standards that the electronic storage media must satisfy to be considered an acceptable method of storage under Rule 17a–4.*[2] [emphasis added]

Further, the SEC issued two Interpretive Releases (No. 34-44238 on May 1, 2001, and No. 34-47806 on May 7, 2003), which pertain specifically to the electronic storage media requirements of paragraph (f).

For additional information, refer to Section 5.1, Overview of SEC Rule 17a-4(f) Electronic Records Storage Requirements.

1.1.2 FINRA Rule 4511(c) Requirements

Financial Industry Regulatory Authority (FINRA) Rule 4511(c) explicitly defers to the format and media requirements of SEC Rule 17a-4, for the books and records it requires.

> *All books and records required to be made pursuant to the FINRA rules shall be preserved in a format and media that complies with SEA [Securities Exchange Act] Rule 17a-4.*

---

[1] Regulators use the phrase *books and records* to describe information about certain business transactions, customers, personnel and other administrative activities that must be retained. Accordingly, Cohasset has used the term Recovery Points (versus *data* or *object*) to consistently recognize that the Recovery Point contains required records.

[2] Exchange Act Release No. 38245 (Feb. 5, 1997), 62 FR 6470 (Feb. 12, 1997) ("Adopting Release").

1.1.3 CFTC Rule 1.31(c)-(d) Requirements

Effective August 28, 2017, 17 CFR § 1.31 (the CFTC Rule), the Commodity Futures Trading Commission (CFTC) promulgated principles-based requirements for organizations electing to retain electronic regulatory records. These amendments modernize and establish technology-neutral requirements for the *form and manner of retention, inspection and production* of regulatory records.

Refer to Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*, which correlates the CFTC principles-based requirements to the capabilities of AWS Backup. Additionally, refer to Section 5.3, *Overview of CFTC Rule 1.31(c)-(d) Electronic Regulatory Records Requirements*.

1.2 Purpose and Approach

To obtain an independent and objective assessment of the compliance capabilities of AWS Backup for preserving regulated electronic records, Amazon Web Services (AWS) engaged Cohasset Associates, Inc. (Cohasset). As a highly-respected consulting firm, Cohasset has recognized expertise and more than 50 years of experience with the legal, technical and operational issues associated with the records management practices of companies regulated by the SEC and CFTC. Additional information about Cohasset is provided in the last section of this report.

AWS engaged Cohasset to:

- Assess the capabilities of AWS Backup in comparison to the five[3] requirements of SEC Rule 17a-4(f) for the recording, non-rewriteable, non-erasable storage and retention of electronic records; see Section 2, *Assessment of Compliance with SEC Rule 17a-4(f);*
- Associate the principles-based requirements of CFTC Rule 1.31(c)-(d) to the assessed capabilities of AWS Backup; see Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d);* and
- Prepare this Assessment Report, enumerating the results of its assessment.

In addition to applying the information in this Assessment Report, regulated entities must ensure that the combination of its policies, procedures and regulatory submissions, in conjunction with the capabilities of implemented electronic recordkeeping solutions, meet all applicable requirements.

This assessment represents the professional opinion of Cohasset and should not be construed as either an endorsement or a rejection, by Cohasset, of AWS Backup and its capabilities or other AWS products or services. The information utilized by Cohasset to conduct this assessment consisted of: (a) oral discussions, (b) system documentation, (c) user and system administrator guides, and (d) other directly-related materials provided by AWS or obtained from publicly available resources.

The content and conclusions of this assessment are not intended, and must not be construed, as legal advice. Relevant laws and regulations constantly evolve, and legal advice is tailored to the specific circumstances of the organization. Therefore, nothing stated herein should be substituted for the advice of competent legal counsel.

---

[3] This assessment of the AWS Backup capabilities focuses on the five requirements of the Rule, effective on the date of this Report, that align with the storage subsystem (a.k.a., electronic recordkeeping system); the remaining requirements of the effective Rule pertain to compliance filings, requirements of the regulated entity, and capabilities of the source system (i.e., the controlling application that utilizes AWS Backup).

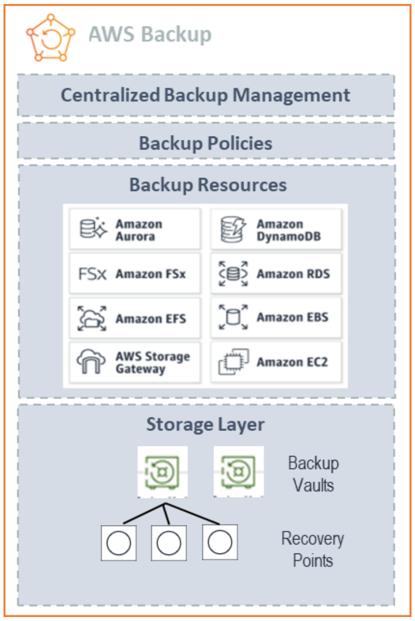
1.3 AWS Backup Overview and Assessment Scope

1.3.1 AWS Backup Overview

AWS Backup is a fully-managed data protection service across AWS services. Using this service, regulated entities can configure backup policies and monitor activity for their AWS resources in one place. It allows regulated entities to automate and consolidate backup tasks that were previously performed service-by-service, and removes the need to create custom scripts and manual processes. AWS Backup is configured to store unique timed backups (Recovery Points) of an AWS Resource. A Recovery Point is a point-in-time view of the resource.

Recovery Points are created and managed according to a Backup Policy that is associated with the resource. The Backup Policy defines the frequency and retention period for each Recovery Point. Further, the Backup Vault can be configured with AWS Backup Vault Lock (*Vault Lock*). Enabling and properly configuring *Vault Lock* (which includes setting *Compliance* mode) applies integrated control codes that place additional restrictions on the actions that can be performed on a Recovery Point and its associated metadata, to prevent erasure prior to the expiration of an assigned retention period.

The hierarchy of the AWS Backup service is summarized as follows:



- **Centralized Backup Management** is (a) the capability to centrally manage Backup Policies and apply the policies to AWS resources across AWS accounts and Regions and (b) the capability to monitor backup activities and demonstrate compliance with controls and reports.
- **Backup Policies** define when and which AWS resources are backed up and for how long the Recovery Points must be retained. For compliance with the Rule, a Backup Policy must be configured with an appropriate retention period (*DeleteAfterDays*) that is between the Min/Max for the Backup Vault where the Recovery Point will be stored. The Backup Policy, together with an appropriately configured *Vault Lock* set to *Compliance* mode, prevents deletion of the Recovery Point and prevents modifying the assigned retention period.
- **Backup Resources** are AWS services and third-party applications that are supported by AWS Backup, including Amazon Elastic Compute Cloud (Amazon EC2) instances, Windows Volume Shadow Copy Service (VSS), Amazon Elastic Block Store (Amazon EBS) volumes, Amazon Relational Database Service (Amazon RDS) databases (including Amazon Aurora clusters), Amazon DynamoDB tables, Amazon Simple Storage Service (S3), Amazon Elastic File System (Amazon EFS) file systems, Amazon FSx for Lustre file systems, Amazon FSx for NetApp ONTAP, Amazon FSx for OpenZFS, Amazon FSx for Windows File Server file systems, VMware Cloud on AWS and AWS Outposts, and AWS Storage Gateway volumes.
- **Backup Vaults** securely store Recovery Points separate from the resource instance. For compliance with the Rule, the Backup Vault must be appropriately configured with *Vault Lock*.

- A **Recovery Point** is a point-in-time snapshot of a resource, which may contain the regulated records. Throughout the letter, Recovery Points is used to describe the AWS resource and all regulated records that are contained within the snapshot of the resource.

1.3.2 AWS Backup Assessment Scope

This assessment report focuses on AWS Backup and stored Recovery Points when (a) the *Vault Lock* feature is enabled and appropriately configured, which includes setting *Vault Lock* and (b) the Backup Policy is configured to apply an appropriate retention period (*DeleteAfterDays)*. When properly configured, these two features are designed to meet the SEC Rule 17a-4(f) requirements, to preserve Recovery Points as non-rewriteable, non-erasable for the required retention period.

2 | Assessment of Compliance with SEC Rule 17a-4(f)

This section presents Cohasset's assessment of the capabilities of Amazon Web Services (AWS) Backup for compliance with the five requirements related to recording and non-rewriteable, non-erasable storage of electronic records, as stipulated in SEC Rule 17a-4(f), effective as of the date of this Report.

For each of the five relevant requirements in SEC Rule 17a-4(f), this assessment is organized into the following four topics:

- ***Compliance Requirement*** – Excerpt of each electronic storage requirement in SEC Rule 17a-4(f) and Cohasset's interpretation of the requirement
- ***Compliance Assessment*** – Assessment of the relevant capabilities of AWS Backup
- ***AWS Backup Capabilities*** – Description of relevant capabilities
- ***Additional Considerations*** – Additional considerations related to meeting the specific requirement

The following subsections document Cohasset's assessment of the capabilities of AWS Backup, as described in Section 1.3, *AWS Backup Overview and Assessment Scope*, relative to each pertinent requirement of SEC Rule 17a-4(f), effective as of the date of this Report. See Section 5.1, *Overview of SEC Rule 17a-4(f) Electronic Records Storage Requirements*, which notates the amended Rule effective January 3, 2023, with a compliance date of May 3, 2023.

2.1 Non-Rewriteable, Non-Erasable Record Format

2.1.1 Compliance Requirement [SEC 17a-4(f)(2)(ii)(A)]

SEC 17a-4(f)(2)(ii)(A): Preserve the records exclusively in a non-rewriteable, non-erasable format

As set forth in Section III(B) of the 2001 Interpretive Release, this requirement *"is designed to ensure that electronic records are capable of being accurately reproduced for later reference by maintaining the records in an unalterable form [for the required retention period]."*

The following statement in the 2003 Interpretive Release further clarifies that certain implementations of rewriteable and erasable media, such as magnetic disk or magnetic tape, meet the requirements of a non-rewriteable, non-erasable recording environment provided: (a) the storage solution delivers the prescribed functionality and (b) the functionality is delivered via appropriate integrated control codes for the SEC designated retention period associated with the stored records.

> *A broker-dealer would not violate the requirement in paragraph (f)(2)(ii)(A) of the rule if it used an electronic storage system that prevents the overwriting, erasing or otherwise altering of a record during its required retention period through the use of integrated hardware and software control codes.* [emphasis added]

Further, Section IV of the 2003 Interpretive Release places requirements on the storage system for retaining records beyond the SEC-established retention period when certain circumstances occur, such as a subpoena or legal hold:

> *Moreover, there may be circumstances (such as receipt of a subpoena) where a broker-dealer is required to maintain records beyond the retention periods specified in Rule 17a-4 or other applicable Commission rules. Accordingly, a broker-dealer must take appropriate steps to ensure that records are not deleted during periods when the regulatory retention period has lapsed but other legal requirements mandate that the records continue to be maintained, and the broker-dealer's storage system must allow records to be retained beyond the retentions periods specified in Commission rules.* [emphasis added]

This statement by the SEC clarifies that the storage system must have the capability to retain records beyond the retention period established at the time of initial recording when required for legal matters, external investigations or audits, or other similar circumstances.

This assessment pertains to the non-erasable, non-rewriteable (a.k.a. WORM or write-once, read-many) requirement, which is specified in both (a) the current Rule effective as of the date of this Report and (b) the amended Rule effective January 3, 2023. This assessment report does not address the audit-trail alternative to WORM, as specified in the amended Rule effective January 3, 2023, with a compliance date of May 3, 2023.

2.1.2 Compliance Assessment

It is Cohasset's opinion that AWS Backup, when *Vault Lock* is set to *Compliance* mode, meets this SEC requirement to retain required records in non-rewriteable, non-erasable format for time-based[4] retention periods and any legal hold, when (a) properly configured, as described in Section 2.1.3 and (b) the considerations described in Section 2.1.4 are satisfied.

2.1.3 AWS Backup Capabilities

This section describes the capabilities of AWS Backup that directly pertain to this SEC requirement for preserving Recovery Points, containing required records, as non-rewriteable, non-erasable for the required retention period.

2.1.3.1 *Definitions*

- **Recovery Point** retention period is derived from the backup policy that generated it, on the frequency specified in the policy, and the retention period is stored as an attribute of the Recovery Point. Thus, changing the backup policy will not impact previously created Recovery Points.
- **Records**[5] are stored in Recovery Points. Cohasset recommends records be stored within 24 hours of creation. Accordingly, Cohasset recommends that Recovery Points be generated within 24 hours of record creation and that each Recovery Point be utilized to retrieve the associated records. Subsequent Recovery Points may

---

[4] Time-based retention periods require records to be retained for a specified contiguous period of time from the date and time created and stored.

[5] Regulators use the phrase *books and records* to describe information about certain business transactions, customers, personnel and other administrative activities that must be retained. Accordingly, Cohasset has used the term Recovery Points (versus *data* or *object*) to consistently recognize that the Recovery Point contains required records.

include prior days' records; however, the longer the timespan from record creation to Recovery Point capture may result in the Recovery Point containing records that have been changed or missing records that have been deleted.

2.1.3.2 *Overview*

The AWS Backup provides the centralized management of AWS resources for Recovery Points and associated metadata on the AWS cloud infrastructure.

To meet this SEC Rule 17a-4(f) requirement:

- AWS Backup *Vault Lock* feature must be enabled (True), the *Vault Lock* must be set to *Compliance* mode, and the configuration grace time must have expired for the *Backup Vault*. See the Subsection 2.1.3.3, *Vault Lock Configuration*, below, for additional information.
- A Backup policy must be configured to (a) store Recovery Points with the *Vault Lock* set to *Compliance* mode and (b) apply an appropriate *DeleteAfterDays* (retention period) to each Recovery Point.

The fundamental features of AWS Backup prevent changes or modifications to a Recovery Point and its immutable metadata, once stored. Further, when the above configurations and settings are made and the grace time has expired:

- The *Vault Lock* configuration cannot be changed or removed:
  - The *Vault Lock* enabled (True) cannot be reset or removed.
  - The *Compliance* mode cannot be changed or removed.
  - The Min/Max cannot be changed or removed.
- The Recovery Point, and its immutable metadata, cannot be overwritten or deleted until the applied *DeleteAfterDays* (retention period) has expired.
  - These settings prevent all (a) user-initiated actions, via any Amazon API (application program interface) request, AWS CLI (command-line interface), SDK (software development kit), or the AWS Backup console (Console), as well as (b) lifecycle policies from overwriting or deleting the Recovery Points before the *DeleteAfterDays* has expired.

2.1.3.3 *Vault Lock Configuration*

To be compliant with the Rule, a Backup Vault must be properly configured as *Locked* in *Compliance* mode, which requires the following:

1. *Backup Vault Name*: The name of the Backup Vault to Lock.
2. *Locked:* The enablement of the *Vault Lock* feature, must be set to True.
3. *Vault Lock*: Must be set to *Compliance* mode.
   - When using the API/CLI, the *Vault Lock* defaults to *Compliance* mode.
   - When using the Console, the administrator must select *Compliance* mode when presented with the options of: (1) *Compliance* mode and (2) *Governance* mode.

  - ◆ IMPORTANT NOTE: The *Vault Lock* mode **must** be set to *Compliance* mode, for Recovery Points required for compliance with SEC Rule 17a-4(f), which disallows users, including the account root user, from shortening or removing the *DeleteAfterDays*.

4. *MaxRetentionDays*: The maximum retention period that the vault retains Recovery Points. If a backup job attempts to store a Recovery Point with a retention period (*DeleteAfterDays*) longer than the maximum retention period, it will fail and an error will be logged.
5. *MinRetentionDays:* The minimum retention period that the vault retains Recovery Points. If a backup job attempts to store a Recovery Point with a retention period (*DeleteAfterDays*) shorter than the minimum retention period, it will fail and an error will be logged.
6. *ChangeableForDays (Vault Lock start date)*: The cooling off period of time during which the *Vault Lock* may be removed, which is only configured for *Compliance* mode.
   - ◆ When the grace time is valid (not yet expired) or set to indefinite (null), the *Vault Lock* features may be changed or disabled. Therefore, the Vault is <u>not</u> in a compliant state during this period.
   - ◆ Once the grace time has expired, the Vault is *Locked* in *Compliance* mode and is in a compliant state:
     - ■ The *Vault Lock* enablement (True) and the *Compliance* mode cannot be changed or removed.
     - ■ The Backup Vault *Minimum* and *Maximum* retention periods cannot be changed.

2.1.3.4 ***<u>Recovery Points Definitions and Retention Controls</u>***

- ▶ A Recovery Point is a point-in-time view of the resource and is inherently *read-only* and therefore immutable.
  - ● Immutable metadata applied to the Recovery Point, includes, but is not limited to: Backup Vault Name, recoveryPoint Amazon Resource Name (ARN), backup date/time, and user-defined custom metadata (key-value pairs).
  - ● The Retention period (DeleteAfterDays) applied to the Recovery Point is immutable when the *Vault Lock* is set to *Compliance* mode and the *Vault Lock* grace time is expired.
- ▶ Retention controls are applied by a *Backup Policy,* configured with *Backup Rules,* that define the following backup criteria: (1) AWS Resource, (2) Frequency, (3) Backup Vault Name, (4) Lifecyle setting, and (5) Resource assignment (AWS Identity and Access Management (IAM) role).
  - ◆ When configuring an advanced lifecycle attribute in the Backup Policy, the *DeleteAfterDays*, must be configured with an appropriate retention period to ensure the Recovery Points are retained in compliance with regulatory requirements.
    - ■ The *DeleteAfterDays* applied to a Recovery Point cannot be changed or deleted when a Backup Vault is *Locked* in *Compliance* mode and the *Vault Lock* grace time has expired.
- ▶ The following AWS Backup features prevent modification, overwrite and deletion, until eligible.
  - ● Recovery Points are inherently *read-only* and therefore are immutable.

  - Each Recovery Point is protected from deletion, by users and by lifecycle policies, when the retention period (*DeleteAfterDays)* for the Recovery Point has not expired. Further, when *Vault Lock* is set to *Compliance* mode, the retention period (*DeleteAfterDays)* cannot be changed or removed.
  - Additionally, an active Hold applied to the recovery point mandates ongoing retention; see subsection 2.1.3.5, *Legal Holds (Temporary Holds),* below.
- A Recovery Point may be copied to a different Backup Vault, resulting in the creation of a new (separate) Recovery Point with its own unique metadata, including the assignment of a new *DeleteAfterDays*. The original Recovery Point and its metadata remains, unaltered, in the original Backup Vault, until deletion.
- If the user or Lifecycle Policy attempts the following, an appropriate error and event is logged, and the action is rejected:
  - Set a retention period (*DeleteAfterDays)* that is outside the Minimum and Maximum range applied to the *Locked Vault* where the Recovery Point is stored.
  - Modify the retention period of a Recovery Point stored in a Backup Vault configured with the *Vault Lock* set to *Compliance* mode.
  - Delete a Recovery Point before the retention period has expired.

2.1.3.5 ***Legal Holds (Temporary Holds)***

When litigation or a subpoena requires records to be placed on hold, which could entail retaining them beyond their assigned retention period, the regulated entity must ensure the subject records (contained in associated Recovery Points) are protected for the duration of the hold.

- Holds are created and applied by selecting the Resource, Recovery Points and date range subject to the hold. Optionally, Hold tags may be applied to categorize and facilitate managing the hold.
  - Once the *Legal Hold* is created and applied (“Active”), it cannot be modified, it can only be released.
  - NOTE: Multiple holds may be applied to a Recovery Point.
  - While an active *Legal Hold* applies to a Recovery Point, overwriting and deleting the Recovery Point is prohibited, even if the associated retention period has expired.
- Holds are released by retrieving the Hold (viewing the Hold details) and selecting and confirming the release Hold option.
  - When a Hold is released, it no longer mandates preservation of the associated Recovery Points, though other active Holds may apply to the Recovery Point, mandating retention.
- Additionally, other retention controls continue to apply to the Recovery Point.
- The Hold status can be verified in the *Legal Hold* user interface, which displays *Hold title*, *Status*, *Description*, *Legal Hold ID*, *Creation Date* and *Release Date*.

2.1.3.6 *Deletion Controls*

- The Recovery Point will be systematically deleted when the *DeleteAfterDays* has passed (expired), if the Recovery Point is not subject to an active Hold. The deletion of a Recovery Point, when eligible, does not impact the recoverability of any Recovery Points still under retention.
- An error is logged, and the action is rejected if the user attempts to delete a Recovery Point when the *DeleteAfterDays* has not passed (expired) or an active legal hold applies.
- A *Locked Vault* cannot be deleted until all Recovery Points stored in the Backup Vault have been deleted.

2.1.3.7 *Clock Management*

- To meet the requirements of the Rule, Cohasset asserts that every system clock must synchronize to an external time server, e.g., a network time protocol (NTP) clock.
- The Amazon Backup system clocks regularly and frequently check the time of the external source and resynchronize. Neither end users nor system administrators have the ability to manipulate system time. These controls prevent or correct any inadvertent or intentional administrative modifications of the time clock, which could allow for premature deletion of Recovery Points.

2.1.3.8 *Security*

- Amazon Web Services are designed to meet Enterprise security and compliance requirements.
- Amazon protects data in transit using SSL/TLS, as well as at rest (data stored on disks in Amazon data centers) using a variety of encryption methods.
- Access to AWS Backup requires credentials, which must have permissions to access AWS resources, such as Backup Vaults, Recovery Points, Backup Policies and Holds. Moreover, Recovery Points created by AWS Backup cannot be deleted using the source service (such as Amazon EFS). Instead, deletion eligible Recovery Points can be deleted only using AWS Backup services.
- AWS Backup supports encryption for Recovery Points (backups) and copies of the backups.

2.1.4 Additional Considerations

To assure compliance with the non-rewriteable, non-erasable requirements of the SEC Rule, the regulated entity is responsible for:

- Properly configuring Backup Vaults used to store Recovery Points required to be compliant with the Rule:
  - Enabling the *Vault Lock* feature (setting to True) and setting *Vault Lock* to *Compliance* mode,
  - Configuring the *MaxRetentionDays,* and *MinRetentionDays* to establish appropriate guardrails for the retention periods applied to Recovery Points, and
  - Configuring a grace time (*ChangeableForDays*) that expires before the Backup Vault stores Recovery Points containing regulated records.
- Configuring Backup Policies with the appropriate retention period (*DeleteAfterDDays).*

- Creating and applying Holds, as appropriate to preserve Recovery Points needed for legal matters, government investigations, external audits and other similar circumstances. Releasing Holds, when appropriate.
- Ensuring that Recovery Points required to comply with the Rule are stored in the properly configured Backup Vault after the grace time has expired, which establishes a *Vault Lock* that cannot be changed or removed.
- Cohasset recommends that Recovery Points, containing regulated records, be generated within 24 hours to help assure accurate and complete records are captured. Subsequent Recovery Points may include prior day's records; however, the longer timespan from record creation to Recovery Point capture may result in the Recovery Point containing records that have been changed or missing records that have been deleted.

Additionally, the regulated entity is responsible for (a) maintaining their AWS Management Account, (b) paying for appropriate services, and (c) procedurally prohibiting users from closing Member Accounts until either (1) the *DeleteAfterDays* has expired on Recovery Points stored in the associated Vaults or (2) until the Recovery Points have been transferred to another compliant storage solution.

2.2 Accurate Recording Process

2.2.1 Compliance Requirement [SEC 17a-4(f)(2)(ii)(B)]

SEC 17a-4(f)(2)(ii)(B): Verify automatically the quality and accuracy of the storage media recording process

The intent of this requirement is to ensure both the accuracy and quality of the recording process such that the records read from the storage media are precisely the same as those that were recorded. This requirement includes both a quality verification of the recording process and post-recording verification processes.

2.2.2 Compliance Assessment

Cohasset affirms that the current capabilities of AWS Backup, in conjunction with the inherent capabilities of advanced magnetic storage technology, meet this SEC requirement for accurate recording and post-recording verification.

2.2.3 AWS Backup Capabilities

AWS Backup has a combination of recording and post-recording verification processes, which are described in the following subsections.

2.2.3.1 *Recording Process*

- AWS Backup utilizes advanced electronic recording technology which applies a combination of checks and balances to assure that Recovery Points are created in a high quality and accurate manner.
- Upon backup completion, the integrity of the Recovery Point data is validated by comparing a SHA256 summary checksum of the full primary resource against AWS Backup's representation of the resources.

2.2.3.2 *Post-Recording Verification*

- AWS Backup is designed to use the AWS global infrastructure to replicate Recovery Points across multiple Availability Zones for durability of 99.999999999% (11 nines) in any given year.
- AWS Backup Audit Manager provides evidence of AWS Backup activities via automatically generated reports and configurable compliance controls.
- AWS regularly verifies the integrity of data stored using checksums. If AWS detects data corruption, it is repaired using redundant data.
- AWS also calculates checksums on all network traffic to detect corruption of data packets when storing or retrieving data.

2.2.4 Additional Considerations

There are no additional considerations related to this requirement.

2.3 Serialize the Original and Duplicate Units of Storage Media

2.3.1 Compliance Requirement [SEC 17a-4(f)(2)(ii)(C)]

This requirement, according to Section III(B) of the SEC's 2001 Interpretive Release, *"is intended to ensure both the accuracy and accessibility of the records by indicating the order in which records are stored, thereby making specific records easier to locate and authenticating the storage process."*

SEC 17a-4(f)(2)(ii)(C): Serialize the original and, if applicable, duplicate units of storage media, and time-date for the required period of retention the information placed on such electronic storage media

When the SEC Rule was issued in 1997, this requirement was thought to be more pertinent to tracking the individual units of removable media related to micrographic or optical storage. This requirement for non-unitized electronic storage may be satisfied by capturing and storing immutable metadata, associated with each electronic record, to *uniquely* identify the record and the *date and time of recording*.

2.3.2 Compliance Assessment

It is Cohasset's opinion that AWS Backup meets this SEC requirement to serialize the original and duplicate records.

2.3.3 AWS Backup Capabilities

- AWS Backup serializes each Recovery Point through a combination of: Backup Vault Name, recoveryPoint Amazon Resource Name (ARN), and backup date/time. These attributes are immutable.
- The combination of the Backup Vault Name, ARN and backup date/time provide a serialization of each Recovery Point in both space and time.

2.3.4 Additional Considerations

There are no additional considerations related to this requirement.

2.4 Capacity to Download Indexes and Records

2.4.1 Compliance Requirement [SEC 17a-4(f)(2)(ii)(D)]

This requirement necessitates an adequate capacity to readily download records and associated indexes, in a format and on a medium acceptable under the Rule and as specified by the SEC or self-regulatory organization. This allows the SEC or self-regulatory organizations to take possession of the downloaded records and indexes.

SEC 17a-4(f)(2)(ii)(D): Have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable under this paragraph (f) as required by the Commission or the self-regulatory organizations of which the member, broker, or dealer is a member

2.4.2 Compliance Assessment

It is Cohasset's opinion that AWS Backup meets this SEC requirement to readily download records and indexes (metadata attributes), when the considerations described in Section 2.4.4 are addressed.

2.4.3 AWS Backup Capabilities

- Recovery Points and metadata (index) attributes may be listed using the AWS Backup console. The Recovery Points may be viewed, either: (1) for a particular AWS resource or (2) all Recovery Points in a single Backup Vault.
- Recovery Points may be restored using specific parameters dependent on the resource type. For each restore, a job is created with a unique job ID. Once the Recovery Point is restored, the applicable records can be extracted using local resources and provided to the examining authority.

2.4.4 Additional Considerations

The regulated entity is responsible for (a) maintaining its account in good standing, (b) maintaining hardware and software to access AWS Backup, (c) maintaining its encryption keys that have been used, and (d) assuring that the regulator, self-regulatory organization or designated examining authority receive downloads of the records and metadata (index) attributes, in the requested format and medium.

2.5 Duplicate Copy of the Records Stored Separately

2.5.1 Compliance Requirement [SEC 17a-4(f)(3)(iii)]

The intent of this requirement is to provide an alternate source for accessing the records, should the primary source be compromised, i.e., lost or damaged.

SEC 17a-4(f)(3)(iii): Store separately from the original, a duplicate copy of the record stored on any medium acceptable under § 240.17a-4 for the time required

Note: A *duplicate copy* is defined as a persistent copy that allows the complete and accurate record to be reestablished from data stored on a compliant storage system or medium. Whereas, a *backup copy* is defined as a non-persistent copy that is overwritten as it is *rotated* on a periodic basis, resulting in a much shorter retention period than the original.

2.5.2 Compliance Assessment

Cohasset affirms that the current capabilities of AWS Backup meet this SEC requirement for a persistent duplicate copy of the Recovery Points, when properly configured, as described in Section 2.5.3.

2.5.3 AWS Backup Capabilities

- Using AWS Backup, the Recovery Points can be copied automatically across AWS accounts within an organization or to multiple different AWS Regions as part of a scheduled backup plan.
- When configuring the secondary Backup Vault, the *Vault Lock* must be set to *Compliance* mode. Further, the Backup policies, specifically the *DeleteAfterDays,* must match between the primary and secondary vaults to ensure a duplicate copy of all Recovery Points are maintained for the same duration and protections as the Recovery Points in the primary Vault.
- All Backups statuses can be monitored through the AWS Backup console to ensure they are properly protected.

2.5.4 Additional Considerations

There are no additional considerations related to this requirement.

3 | Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)

The objective of this section is to document Cohasset's assessment of the capabilities of AWS Backup, as described in Section 1.3, *AWS Backup Overview and Assessment Scope*, in comparison to the CFTC requirements.

The individual relevant requirements cited in Section 2, *Assessment of Compliance with SEC Rule 17a-4(f)*, are based on the wording in SEC Rule 17a-4(f) and Cohasset's interpretation of the requirements, given the associated SEC Interpretive Releases. Specifically, the SEC's 2003 Interpretive Release reiterates that the Rule sets forth standards that the electronic storage media must satisfy to be considered an acceptable method of storage under SEC Rule 17a-4:

> *A broker-dealer would not violate the requirement in paragraph (f)(2)(ii)(A) of the rule if it used an electronic storage system that prevents the overwriting, erasing or otherwise altering of a record during its required retention period through the use of <u>integrated</u> hardware and software <u>control codes</u>.* [emphasis added]

Accordingly, it is Cohasset's opinion that the requirements set forth in SEC Rule 17a-4(f) are *technology-neutral* and apply to any electronic solution with (a) integrated control codes that extend to the electronic storage system and (b) features that deliver capabilities that meet the requirements of the Rule.

The August 28, 2017, amendments to CFTC Rule 1.31 establish *technology-neutral*, *principle-based* requirements. As illustrated in the table in this section, it is Cohasset's opinion that the requirements of the modernized CFTC Rule may be achieved by meeting the SEC requirements.

When comparing the capabilities of AWS Backup that align with the SEC requirements to the *principles-based* CFTC requirements, it is essential to recognize that the SEC Rule separately describes requirements for index data and audit trail, whereas the CFTC in 17 CFR § 1.31(a) establishes an expanded definition of an *electronic regulatory record* to include the information as specified in paragraph (i) and (ii) below.

> ***Definitions**. For purposes of this section:*
> *<u>Electronic regulatory records</u> means all regulatory records other than regulatory records exclusively created and maintained by a records entity on paper.*
> *<u>Records entity</u> means any person required by the Act or Commission regulations in this chapter to keep regulatory records.*
> *<u>Regulatory records</u> means all books and records required to be kept by the Act or Commission regulations in this chapter, including any record of any correction or other amendment to such books and records, provided that, <u>with respect to such books and records stored electronically, regulatory records shall also include:</u>*
> *<u>(i) Any data necessary to access, search, or display any such books and records; and</u>*
> *<u>(ii) All data produced and stored electronically describing how and when such books and records were created, formatted, or modified</u>.* [emphasis added]

The focus of Cohasset's assessment, presented in Section 2, pertains to AWS Backup when *Vault Lock* is set to *Compliance* mode, which is a highly restrictive configuration that assures the storage solution applies integrated controls to (a) protect immutability of the record content and certain system metadata and (b) prevent deletion over the applied retention period.

In the following table, Cohasset correlates the capabilities of AWS Backup when *Vault Lock* is set to *Compliance*, to the *principles-based* CFTC requirements related to the *form and manner of retention* and the *inspection and production of regulatory records*. In addition, Cohasset contends that AWS Backup when *Vault Lock* is set to *Governance* mode, meets these *principles-based* CFTC requirements, when the regulated entity applies appropriate procedural controls to oversee operations that may allow content to be modified or deleted prior to expiration of the retention period. This less restrictive *Governance* configuration provides flexibility to remove or shorten retention periods, which may be beneficial for compliance with privacy and data protection requirements.

The left-hand column lists the *principles-based* CFTC requirements. The middle column provides Cohasset's analysis and opinion regarding the ability of AWS Backup to meet the requirements for electronic regulatory records in CFTC Rule 1.31(c)-(d). In addition, for ease of reference, the right-hand column lists the correlated SEC requirements.

CFTC 1.31(c)-(d) Requirement	Compliance Assessment Relative to CFTC 1.31(c)-(d)	SEC 17a-4(f) Requirements Listed in the Referenced Sections
(c) Form and manner of retention. Unless specified elsewhere in the Act or Commission regulations in this chapter, all regulatory records must be created and retained by a records entity in accordance with the following requirements: (1) **Generally**. Each records entity shall retain regulatory records in a form and manner that ensures the *authenticity and reliability* of such regulatory records in accordance with the Act and Commission regulations in this chapter. (2) **Electronic regulatory records**. Each records entity maintaining electronic regulatory records shall establish appropriate systems and controls that ensure the *authenticity and reliability* of electronic regulatory records, including, without limitation: (i) Systems that *maintain* the security, signature, and data as necessary to ensure the *authenticity* of the information contained in electronic regulatory records and to monitor compliance with the Act and Commission regulations in this chapter;	It is Cohasset's opinion that AWS Backup capabilities, utilized with the *Vault Lock*, as described in Sections 2.1 through 2.4 meet CFTC requirements (c)(1) and (c)(2)(i) for records. Additionally, for *records stored electronically*, the CFTC has expanded the definition of *regulatory records* in 17 CFR § 1.31(a) to include metadata: *Regulatory records means all books and records required to be kept by the Act or Commission regulations in this chapter, including any record of any correction or other amendment to such books and records, provided that, with respect to such books and records stored electronically, regulatory records shall also include:* *(i) Any data necessary to access, search, or display any such books and records; and* *(ii) All data produced and stored electronically describing how and when such books and records were created, formatted, or modified*. [emphasis added] It is Cohasset's opinion that AWS Backup retains immutable metadata attributes (e.g., Backup Vault Name, recoveryPoint ARN, backup date/time, and Retention Period), as an integral part of the Recovery Point. The Recovery Point attributes are subject to the same retention protections as the associated Recovery Point itself. To satisfy this requirement for other essential data related to how and when the Recovery Points were created, formatted, or modified, the regulated entity must retain this data in a compliant manner.	**Section 2.1 *Non-Rewriteable, Non-Erasable Record Format*** *Preserve the records exclusively in a non-rewriteable, non-erasable format* **Section 2.2 *Accurate Recording Process*** *Verify automatically the quality and accuracy of the storage media recording process* **Section 2.3 Serialize the Original and Duplicate Units of Storage Media** *Serialize the original and, if applicable, duplicate units of storage media, and time-date for the required period of retention the information placed on such electronic storage media* ***Section 2.4 Capacity to Download Indexes and Records*** *Have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable under this paragraph (f) as required by the Commission or the self-regulatory organizations of which the member, broker, or dealer is a member*
(ii) Systems that ensure the records entity is able to produce electronic regulatory records[6] in accordance with this section, and *ensure the availability of such regulatory records in the event of an emergency or other disruption* of the records entity's electronic record retention systems; and	It is Cohasset's opinion that AWS Backup capabilities described Section 2.5, including options for duplicating or replicating the Recovery Points meet the CFTC requirements (c)(2)(ii) to *ensure the availability of such regulatory records in the event of an emergency or other disruption of the records entity's electronic record retention systems*. To satisfy this requirement for other essential data that is not retained in AWS Backup (such as separate indices), the regulated entity must retain this other data in a compliant manner.	***Section 2.5 Duplicate Copy of the Records Stored Separately*** *Store separately from the original, a duplicate copy of the record stored on any medium acceptable under §240.17a-4 for the time required*

---

[6] 17 CFR § 1.31(a) includes indices (*Any data necessary to access, search, or display any such books and records*) in the definition of regulatory records.

CFTC 1.31(c)-(d) Requirement	Compliance Assessment Relative to CFTC 1.31(c)-(d)	SEC 17a-4(f) Requirements Listed in the Referenced Sections
(iii) The creation and maintenance of an *up-to-date inventory* that identifies and describes each system that maintains information necessary for accessing or producing electronic regulatory records.	The regulated entity is required to create and retain an *up-to-date inventory,* as required for compliance with 17 CFR § 1.31(c)(iii).	N/A
(d) Inspection and production of regulatory records. Unless specified elsewhere in the Act or Commission regulations in this chapter, a records entity, at its own expense, must *produce or make accessible for inspection* all regulatory records in accordance with the following requirements: (1) *Inspection*. All regulatory records shall be open to inspection by any representative of the Commission or the United States Department of Justice. (2) *Production of **paper** regulatory records*. *** (3) *Production of **electronic** regulatory records*. (i) A request from a Commission representative for electronic regulatory records will specify a *reasonable form and medium* in which a records entity must produce such regulatory records. (ii) A records entity must *produce such regulatory records in the form and medium requested promptly*, upon request, unless otherwise directed by the Commission representative. *(4) Production of **original** regulatory records.* ***	It is Cohasset's opinion that AWS Backup has features that support the regulated entity's efforts to comply with requests for inspection or production of Recovery Points and associated system metadata (i.e., index attributes). ● Specifically, it is Cohasset's opinion that Section 2.4, *Capacity to Download Indexes and Records*, describes use of AWS Backup to list and restore Recovery Points to facilitate the download of associated records and the system metadata retained by AWS Backup. As noted in the *Additional Considerations* in Section 2.4.4, the regulated entity is obligated to produce the record and associated metadata, in the form and medium requested. ● If the regulator requests additional data related to how and when the records were created, formatted, or modified, the regulated entity will need to provide this information from appropriate source systems.	***Section 2.4 Capacity to Download Indexes and Records*** *Have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable under this paragraph (f) as required by the Commission or the self-regulatory organizations of which the member, broker, or dealer is a member*

4 | Conclusions

Cohasset assessed the capabilities of AWS Backup, with *Vault Lock* set to *Compliance* mode, in comparison to the five requirements related to the recording and non-rewriteable, non-erasable storage and retention of electronic records, as set forth in the currently effective SEC Rule 17a-4(f) and its associated Interpretive Releases. (See Section 1.3, *AWS Backup Overview and Assessment Scope*.)

Cohasset determined that AWS Backup, when properly configured, has the following capabilities, which meet the regulatory requirements:

- Maintains Recovery Points, which may contain required records, and immutable Recovery Point metadata in non-rewriteable, non-erasable format for time-based retention periods.
- Preserves all selected Recovery Points as immutable and prohibits deletion or overwrites, while an applied Hold is active.
- Prohibits deletion of a Recovery Point and its immutable metadata until the retention period for the Recovery Point, and any associated Hold has expired.
- Verifies the accuracy and quality of the recording process through cryptographic hash values and AWS validation processes, in addition to the inherent capabilities of advanced magnetic storage technology.
- Uniquely serializes each Recovery Point and all duplicate copies with Backup Vault Name, ARN and backup date/time stamp.
- Maintains a minimum of two duplicates of each Recovery Point on a primary and secondary Backup Vault, which allows for lost or damaged Recovery Points to be restored.
- Provides the capacity and tools to: (a) list and view Recovery Points, and (b) restore a Recovery Point for download of the associated records and associated metadata attributes.

Cohasset also correlated the assessed capabilities of AWS Backup, with *Vault Lock* set to *Compliance* mode, to the principles-based electronic records requirements in CFTC Rule 1.31(c)-(d).

Accordingly, Cohasset concludes that AWS Backup, when properly configured, and utilized to retain time-based records, meets the five requirements related to recording and non-rewriteable, non-erasable storage of electronic records as specified in SEC Rule 17a-4(f) and FINRA Rule 4511(c). In addition, the assessed capabilities meet the principles-based electronic records requirements of CFTC Rule 1.31(c)-(d).

5 | Overview of Relevant Regulatory Requirements

This section establishes the context for the regulatory requirements that are the subject of this assessment by providing an overview of the regulatory foundation for allowing electronic records to be retained on a variety of compliant electronic storage media.

5.1 Overview of SEC Rule 17a-4(f) Electronic Records Storage Requirements

Recordkeeping requirements for the securities broker-dealer industry are stipulated by the United States Securities and Exchange Commission (SEC) Regulations, including 17 CFR §§ 240.17a-3 and 240.17a-4. Specifically, SEC Rule 17a-4(f), when adopted on February 12, 1997, expressly allow books and records to be retained on electronic storage media, subject to meeting certain conditions.

Three separate foundational documents collectively define and interpret the specific regulatory requirements that must be met for an electronic storage system to be compliant with SEC Rule 17a-4(f). These are:

- The Rule itself, as modified over time by the SEC. These modifications to the original Rule have not affected the requirements for electronic storage media, which are the basis of this assessment. However, certain Interpretive Releases have clarified the context and meaning of certain requirements and conditions of the Rule.
- SEC Interpretive Release No. 34-44238, Commission Guidance to Broker-Dealers on the Use of Electronic Storage Media under the Electronic Signatures in Global and National Commerce Act of 2000 with Respect to Rule 17a-4(f), dated May 1, 2001 (the 2001 Interpretive Release).
- SEC Interpretive Release No. 34-47806, Electronic Storage of Broker-Dealer Records, dated May 7, 2003 (the 2003 Interpretive Release).

In the Rule and in the two subsequent interpretative releases, the SEC authorizes the use of electronic storage media and devices to satisfy the recordkeeping requirements of SEC Rules 17a-3 and 17a-4, when the system delivers the prescribed functionality. Specifically, SEC Rule 17a-4(f)(1)(ii) states:

> *(f) The records required to be maintained and preserved pursuant to §§ 240.17a-3 and 240.17a-4 may be immediately produced or reproduced on "micrographic media" (as defined in this section) or by means of "electronic storage media" (as defined in this section) that meet the conditions set forth in this paragraph and be maintained and preserved for the required time in that form.*
> *(1) For purposes of this section:*
> *(ii) The term electronic storage media means any digital storage medium or system and, in the case of both paragraphs (f)(1)(i) and (f)(1)(ii) of this section, that meets the applicable conditions set forth in this paragraph (f).* [emphasis added]

The February 12, 1997, Federal Register issued the final rule allowing broker-dealers to use electronic storage media. When issuing the rule, the SEC recognized that technology evolves; and, it set forth standards that the electronic storage media must satisfy, rather than prescribing specific technology, as specified in the following excerpts:

> ***SUMMARY:*** *The Securities and Exchange Commission ("Commission") is amending its broker-dealer record preservation rule to allow broker-dealers to employ, under certain conditions, electronic storage media to maintain records required to be retained. The amendments reflect a recognition of technological developments that will provide economic as well as time-saving advantages for broker-dealers by expanding the scope of recordkeeping options while at the same time continuing to require broker-dealers to maintain records in a manner that preserves their integrity. The Commission is also issuing an interpretation of its record preservation rule relating to the treatment of electronically generated communications.*
>
> ***
>
> ***II. Description of Rule Amendments***
> ***A. Scope of Permissible Electronic***
> ***Storage Media***
>
> ****The Commission is adopting a rule today which, instead of specifying the type of storage technology that may be used, sets forth standards that the electronic storage media must satisfy to be considered an acceptable method of storage under Rule 17a–4. Specifically, because optical tape, CD–ROM, and certain other methods of electronic storage are available in WORM and can provide the same safeguards against data manipulation and erasure that optical disk provides, the final rule clarifies that broker-dealers may employ any electronic storage media that meets the conditions set forth in the final rule.*[7] [emphasis added]

The 2003 Interpretive Release further clarifies that implementation of rewriteable and erasable media, such as magnetic tape or magnetic disk, meets the requirements of a non-rewriteable, non-erasable recording environment, if the system delivers the prescribed functionality and appropriate **integrated control codes** are in place. The 2003 Interpretive Release states:

> *A broker-dealer would not violate the requirement in paragraph (f)(2)(ii)(A) of the rule if it used an electronic storage system that prevents the overwriting, erasing or otherwise altering of a record during its required retention period through the use of integrated hardware and software control codes.* [emphasis added]

The key words within this statement are '*integrated*' and '*control codes*'. The term '*integrated*' means that the method used to achieve a non-rewriteable, non-erasable recording environment must be an integral part of the recording hardware and software. The term '*control codes*' indicates the acceptability of using attribute codes (metadata), which are integral to the hardware and software of the recording process, to protect against overwriting or erasure of any records.

Examples of *integrated control codes* relevant to a non-rewriteable, non-erasable recording process are:

- A retention period during which the record cannot be erased, overwritten or otherwise modified;
- A unique record identifier that differentiates each record from all other records; and
- The date and time of recording, which in combination with the unique identifier "serializes" the record.

---

[7] Exchange Act Release No. 38245 (Feb. 5, 1997), 62 FR 6469 (Feb. 12, 1997) ("Adopting Release").

The 2003 Interpretive Release specifically notes that recording processes or applications which merely mitigate the risk of overwrite or erasure (rather than prevent them), such as relying solely on access control security, will not satisfy the requirements of SEC Rule 17a-4(f).

Further, the 2003 Interpretive Release requires the storage system to be capable of retaining records beyond the SEC-established retention period, when required by a subpoena, legal hold or other similar circumstances. In *Section IV. Discussion*, the 2003 Interpretive Release states:

> *Moreover, there may be circumstances (such as receipt of a subpoena) where a broker-dealer is required to maintain records beyond the retention periods specified in Rule 17a-4 or other applicable Commission rules. Accordingly, a broker-dealer must take appropriate steps to ensure that records are not deleted during periods when the regulatory retention period has lapsed but other legal requirements mandate that the records continue to be maintained, and the broker-dealer's storage system must allow records to be retained beyond the retentions periods specified in Commission rules.* [emphasis added]

An important associated requirement of SEC Rule 17a-4(f)(2)(i) is that a member, broker or dealer electing to electronically store its records required by SEC Rules 17a-3 or 17a-4, must notify its designated examining authority at least ninety (90) days prior to employing any technology other than write-once read-many (WORM) optical media. Examining authorities are self-regulatory organizations (SROs) or designated examining authorities (DEAs) under the jurisdiction of the SEC, such as the Financial Industry Regulatory Authority (FINRA).

Important Note: In the November 3, 2022, Federal Register[8], the SEC issued a Final Rule, which amends Rule 17a-4. The amended Final Rule 17a-4 is effective January 3, 2023, with a compliance date of May 3, 2023.

The amendments (a) provide an audit-trail alternative and (b) allow regulated entities to continue using the electronic recordkeeping systems they currently employ to meet the non-erasable, non-rewriteable (a.k.a. WORM or write-once, read-many) requirement, as clarified in the May 7, 2003, Interpretive Release:

> *** the Commission is proposing amendments to Rules 17a-4(f) and 18a-6(e) that would provide firms with the option of using electronic recordkeeping systems that meet either the audit-trail requirement or the WORM requirement. Moreover, as discussed above, the Rule 17a-4(f) Interpretation, which is extant, clarifies that Rule 17a-4(f) does not mandate the use of optical disk to meet the WORM requirement.* [emphasis added]
>
> *****
>
> *Under the proposed amendments, broker-dealers could potentially continue to use the electronic recordkeeping systems they currently employ to meet the WORM requirement. ***** Moreover, some broker-dealers may choose to use their existing WORM-compliant electronic recordkeeping systems rather than adopt a new technology. Further, some broker-dealers may choose to retain existing electronic records on a legacy WORM-compliant electronic recordkeeping system, including software-based systems that are designed to follow the Rule 17a-4(f) Interpretation rather than transfer them to an electronic recordkeeping system that would meet the proposed audit-trail requirement. However, these firms could decide to preserve new records on an electronic recordkeeping system that would meet the proposed audit-trail requirement.*

---

[8] Exchange Act Release No. 34-96034; File No. S7-19-21 (Oct. 12, 2022), 87 FR 66412 (Nov. 3, 2022) ("Final rule").

See Section 2, *Assessment of Compliance with SEC Rule 17a-4(f),* for the five SEC requirements, addressed in this Report, together with a description of the capabilities of AWS Backup related to each requirement. The non-erasable, non-rewriteable (a.k.a. WORM or write-once, read-many) requirement is specified in **both** (a) the current Rule effective as of the date of this Report, and (b) the amended Rule effective January 3, 2023, with a compliance date of May 3, 2023. The other four SEC requirements addressed in this Report, pertain to the Rule effective as of the date of this Report.

5.2 Overview of FINRA Rule 4511(c) Electronic Records Storage Requirements

Financial Industry Regulatory Authority (FINRA) Rule 4511(c) explicitly defers to SEC Rule 17a-4(f), by stipulating:

> *(c) All books and records required to be made pursuant to the FINRA rules shall be preserved in a format and media that complies with SEA [Securities Exchange Act] Rule 17a-4.*

5.3 Overview of CFTC Rule 1.31(c)-(d) Electronic Regulatory Records Requirements

Effective August 28, 2017, the Commodity Futures Trading Commission (CFTC) amended 17 CFR § 1.31 (CFTC Rule) to define principles-based requirements for organizations electing to retain electronic regulatory records. The CFTC requirements for electronic regulatory records evolved through amendments to Rule 1.31. The most substantive changes included:

- The June 28, 1999, amendment first implemented the technical provisions regarding the use of electronic storage media for required books and records.
- The November 2, 2012, amendment clarified the retention period for certain oral communications.
- The August 28, 2017, amendments modernize and make technology-neutral the form and manner in which regulatory records, including electronic regulatory records, must be retained and produced.

To address the transition to electronic regulatory records, the CFTC amended and modernized its recordkeeping regulation to adopt principles-based standards that are less prescriptive. This resulted in rephrasing and modernizing the requirements previously defined in 1999, as explained in the August 28, 2017, Federal Register in *III. Final Rules, D. Regulation 1.31(c): Form and Manner of Retention*:

> *Consistent with the Commission's emphasis on a less-prescriptive, principles-based approach, proposed § 1.31(d)(1) would rephrase the existing requirements in the form of a general standard for each records entity to retain all regulatory records in a form and manner necessary to ensure the records' and recordkeeping systems' authenticity and reliability. The Commission proposed to adopt § 1.31(d)(2) to set forth additional controls for records entities retaining electronic regulatory records. The Commission emphasized in the Proposal that the proposed regulatory text does not create new requirements, but rather updates the existing requirements so that they are set out in a way that appropriately reflects technological advancements and changes to recordkeeping methods since the prior amendments of § 1.31 in 1999.* [emphasis added]

The definitions established in 17 CFR § 1.31(a) are paramount to applying the CFTC requirements.

> *Electronic regulatory records means all regulatory records other than regulatory records exclusively created and maintained by a records entity on paper.*

> *Records entity means any person required by the Act or Commission regulations in this chapter to keep regulatory records.*
> *Regulatory records means all books and records required to be kept by the Act or Commission regulations in this chapter, including any record of any correction or other amendment to such books and records, provided that, with respect to such books and records stored electronically, regulatory records shall also include:*
> *(i) Any data necessary to access, search, or display any such books and records; and*
> *(ii) All data produced and stored electronically describing how and when such books and records were created, formatted, or modified.* [emphasis added]

These definitions establish that recordkeeping obligations apply to (a) all *records entities*, without exception, and (b) all *regulatory records*. Further, for *electronic regulatory records*, paragraphs (i) and (ii) establish an expanded definition of an electronic regulatory record to include information describing data necessary to access, search and display records, as well as information describing how and when such books and records were created, formatted, or modified.

The retention time periods for regulated records includes both time-based and event-time-based retention periods. Specifically, 17 CFR § 1.31(b)(1)-(b)(3) states:

> ***Duration of retention**. Unless specified elsewhere in the Act or Commission regulations in this chapter:*
> *(1) A records entity shall keep regulatory records of any swap or related cash or forward transaction (as defined in § 23.200(i) of this chapter), other than regulatory records required by § 23.202(a)(1) and (b)(1)-(3) of this chapter, from the date the regulatory record was created until the termination, maturity, expiration, transfer, assignment, or novation date of the transaction and for a period of not less than five years after such date.*
> *(2) A records entity that is required to retain oral communications, shall keep regulatory records of oral communications for a period of not less than one year from the date of such communication.*
> *(3) A records entity shall keep each regulatory record other than the records described in paragraphs (b)(1) or (b)(2) of this section for a period of not less than five years from the date on which the record was created.* [emphasis added]

For a list of the CFTC principles-based requirements and a summary assessment of AWS Backup in relation to each requirement, see Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*.

About Cohasset Associates, Inc.

Cohasset Associates, Inc. (www.cohasset.com) is recognized as a leading professional consulting firm, specializing in records management and information governance. Drawing on more than forty years of experience, Cohasset provides its clients with innovative advice on managing their electronic information as the digital age creates operational paradigms, complex technical challenges and unprecedented legal issues.

Cohasset provides award-winning professional services in four areas: management consulting, education, thought-leadership and legal research.

Management Consulting: Cohasset strategizes with its multi-national and domestic clients, engaging in implementation activities to promote interdisciplinary information governance, achieve business objectives, optimize information value, improve compliance, and mitigate information-related risk.

Cohasset has been described as *the only management consulting firm in its field with its feet in the trenches and its eye on the horizon*. This fusion of practical experience and vision, combined with a commitment to excellence, results in Cohasset's extraordinary record of accomplishments.

Education: Cohasset is distinguished through its delivery of exceptional and timely education and training on records and information lifecycle management and information governance.

For domestic and international clients, Cohasset:

- *Formulates information governance implementation strategies*
- *Develops policies and standards for records management and information governance*
- *Creates clear and streamlined retention schedules*
- *Prepares training and communications for executives, the RIM network and all employees*
- *Leverages content analytics to improve lifecycle controls for large volumes of eligible information, enabling clients to classify information, separate high-value information and delete what has expired*
- *Designs and assists with the implementation of information lifecycle practices that avoid the cost and risk associated with over-retention*
- *Defines technical and functional requirements and assists with the deployment of enterprise content management and collaboration tools*

Thought-leadership: Cohasset regularly publishes thought-leadership white papers and surveys to promote the continuous improvement of information lifecycle management practices.

Legal Research: Cohasset is nationally respected for its direction on information governance legal issues – from retention schedules to compliance with the regulatory requirements associated with the use of electronic or digital storage media.

©2022 Cohasset Associates, Inc.

This Assessment Report and the information contained in it are copyrighted and are the sole property of Cohasset Associates, Inc. Selective references to the information and text of this Assessment Report are welcome, provided such references have appropriate attributions and citations. Permission is granted for in-office reproduction so long as the contents are not edited and the *look and feel* of the reproduction is retained.