Cohasset Associates

Amazon® Simple Storage Service™ (S3)

COMPLIANCE ASSESSMENT

SEC 17a-4(f), SEC 18a-6(e), FINRA 4511(c) and CFTC 1.31(c)-(d)

Abstract

Amazon® Simple Storage Service™ (S3), offered on the Amazon Web Services™ (AWS) cloud computing platform, provides industry-leading, highly scalable and secure object storage. The Amazon S3 *Object Lock* feature is designed to meet securities industry requirements for preserving records in non-rewriteable, non-erasable format for the applied retention period and legal holds.

In this report, Cohasset Associates, Inc. (Cohasset) assesses the functionality of Amazon S3 (see Section 1.3, *Amazon S3 Overview and Assessment Scope*) relative to the electronic records requirements, specified by multiple regulatory bodies, as follows:

- Securities and Exchange Commission (SEC) in 17 CFR § 240.17a-4(f)(2);
- SEC in 17 CFR § 240.18a-6(e)(2);
- Financial Industry Regulatory Authority (FINRA) in Rule 4511(c), which defers to the format and media requirements of SEC Rule 17a-4(f); and
- Commodity Futures Trading Commission (CFTC) in 17 CFR § 1.31(c)-(d).

It is Cohasset's opinion that Amazon S3, when properly configured and used with the *Object Lock* feature, has functionality that meets the electronic recordkeeping system requirements of SEC Rules 17a-4(f)(2) and 18a-6(e)(2) and FINRA Rule 4511(c), as well as supports the regulated entity in its compliance with SEC Rules 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii). Additionally, the assessed functionality of Amazon S3 meets the principles-based requirements of CFTC Rule 1.31(c)-(d).

COHASSET'S INDUSTRY INSIGHT AND EXPERIENCE

Core to our practice is the delivery of records management and information governance professional consulting services, and education and training. Cohasset's expert consulting services support regulated organizations, including those in financial services. Cohasset serves both domestic and multi-national clients, aligning information lifecycle controls to their organizations' business priorities, facilitating regulatory compliance and risk mitigation, while generating quantifiable business efficiency.

Cohasset assesses a range of electronic recordkeeping systems, each designed to meet the requirements of the Securities and Exchange Commission Rules 17a-4(f)(2) and 18a-6(e)(2) for record audit-trail and non-rewriteable, non-erasable record formats, considering the SEC 2001, 2003 and 2019 interpretations. For the non-rewriteable, non-erasable record, these interpretations authorize the use of erasable storage, conditioned on integrated software or hardware control codes, to prevent overwriting, erasing, or otherwise altering the records, during the applied retention period.

December 2025

12800 Whitewater Drive, Suite 100
Minnetonka, MN 55343-9347 | USA

+1.312.527.1550 | Visit Cohasset website

Table of Contents

1 • Introduction

Regulators, worldwide, establish explicit requirements for certain regulated entities that elect to electronically retain books and records. Given the prevalence of electronic books and records, these requirements apply to most broker-dealers, commodity futures trading firms and similarly regulated organizations.

This Introduction *summarizes the regulatory environment pertaining to this assessment and the purpose and approach for Cohasset's assessment. It also provides an overview of Amazon S3 and the assessment scope.*

1.1 Overview of the Regulatory Requirements

1.1.1 SEC Rules 17a-4(f) and 18a-6(e) Requirements

In 17 CFR §§ 240.17a-3 and 240.17a-4 for the securities broker-dealer industry and 17 CFR §§ 240.18a-5 and 240.18a-6 for nonbank SBS entities[1], the SEC stipulates recordkeeping requirements, including retention periods.

Effective January 3, 2023, the U.S. Securities and Exchange Commission (SEC) promulgated amendments to 17 CFR § 240.17a-4 (SEC Rule 17a-4) and 17 CFR § 240.18a-6 (SEC Rule 18a-6), which define explicit requirements for electronic storage systems.

> *The Securities and Exchange Commission ("Commission") is adopting amendments to the recordkeeping rules applicable to broker-dealers, security-based swap dealers, and major security-based swap participants. The amendments modify requirements regarding the maintenance and preservation of electronic records****[2] [emphasis added]

For additional information, refer to Section 2, *Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e),* and Appendix A.1, *Overview of SEC Rules 17a-4(f) and 18a-6(e) Electronic Recordkeeping System Requirements*.

1.1.2 FINRA Rule 4511(c) Requirements

Financial Industry Regulatory Authority (FINRA) Rules regulate member brokerage firms and exchange markets. These Rules were amended to address security-based swaps (SBS).[3]

FINRA Rule 4511(c) explicitly defers to the requirements of SEC Rule 17a-4, for 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*. [emphasis added]

---

1 Throughout this report, 'nonbank SBS entity' refers to security-based swap dealers (SBSD) and major security-based swap participants (MSBSP) that are not also registered as a broker-dealer without a prudential regulator.

2 Electronic Recordkeeping Requirements for Broker-Dealers, Security-Based Swap Dealers, and Major Security-Based Swap Participants, Exchange Act Release No. 96034 (Oct. 12, 2022) 87 FR 66412 (Nov. 3, 2022) (2022 Electronic Recordkeeping System Requirements Adopting Release).

3 FINRA, Regulatory Notice 22-03 (January 20, 2022), FINRA Adopts Amendments to Clarify the Application of FINRA Rules to Security-Based Swaps.

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.

For additional information, refer to Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*, and Appendix A.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 Amazon S3 for preserving required electronic records, Amazon engaged Cohasset Associates, Inc. (Cohasset). As a specialized consulting firm, Cohasset has more than fifty 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.

Amazon engaged Cohasset to:

- Assess the functionality of Amazon S3, in comparison to the electronic recordkeeping system requirements of SEC Rules 17a-4(f)(2) and 18a-6(e)(2) and describe audit system features that support the regulated entity in its compliance with SEC Rules 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii); see Section 2, *Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e);*
- Address FINRA Rule 4511(c), given FINRA explicitly defers to the requirements of SEC Rule 17a-4; see Section 2, *Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e);*
- Associate the principles-based requirements of CFTC Rule 1.31(c)-(d) with the assessed functionality of Amazon S3; see Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d);* and
- Prepare this Compliance Assessment Report, enumerating the assessment results.

In addition to applying the information in this Compliance Assessment Report, regulated entities must ensure that the combination of its policies, procedures and regulatory submissions, in conjunction with the functionality of implemented electronic recordkeeping systems, 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 Amazon S3 and its functionality or other Amazon 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) related materials provided by Amazon 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.

1.3 Amazon S3 Overview and Assessment Scope

1.3.1 Amazon S3 Overview

Amazon® Simple Storage Service™ (S3), offered on the Amazon Web Services™ (AWS) cloud computing platform, provides industry leading, highly scalable and secure object[4] storage.

The storage hierarchy of these AWS services is depicted in Figure 1 and summarized below.

- An AWS Organization has one AWS **Management Account** and it may have multiple Organizational Units to group its AWS Member Accounts.
- **Organizational Units** may be nested, allowing **Member Accounts** to be hierarchical and managed centrally.
- A **Member Account** is assigned to one Organization Unit at a time and may have multiple Amazon S3 Buckets, as one of its services.

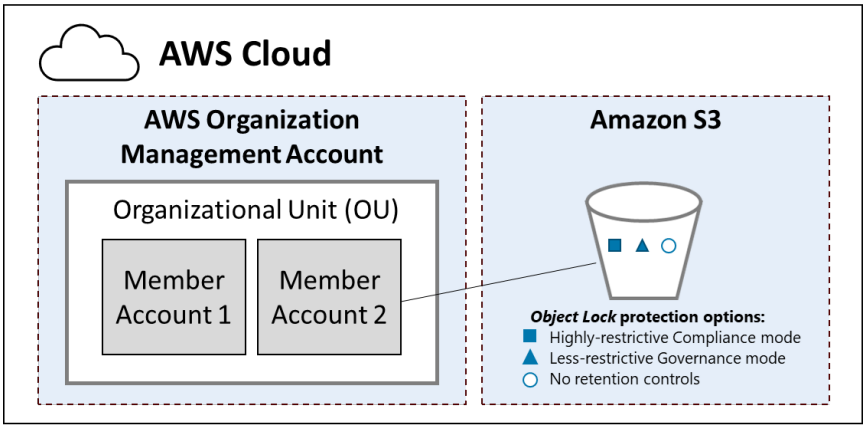

Figure 1: Amazon S3 Storage Hierarchy

Amazon S3 is the storage infrastructure. **Buckets** are public cloud storage resources available in Amazon S3 storage services. Amazon S3 Buckets retain individual versions of objects, which are comprised of the content and descriptive metadata. For Buckets intended to retain required records in compliance with SEC Rules 17a-4(f) and 18a-6(e), the *Object Lock* feature must be enabled, which allows highly-restrictive *Compliance* mode or less-restrictive *Governance* mode retention controls to be applied to stored records.

1.3.2 Assessment Scope

The scope of this assessment is focused specifically on the compliance-related capabilities of Amazon S3, using the *Object Lock* feature in either highly-restrictive *Compliance* mode or less-restrictive *Governance* mode, when deployed on the hosted Amazon Web Services (AWS) platform. Note: When less-restrictive *Governance* mode controls are applied, procedural controls and monitoring are required to scrutinize actions taken by administrators with *BypassGovernanceRetention* permissions, who have the ability to shorten or remove retention controls and prematurely delete required records.

[4] The SEC uses the phrase *books and records* to describe information that must be retained for regulatory compliance. In this report, Cohasset uses the term *record*, in addition to specific terms, e.g., object or version, to recognize that the content may be required for regulatory compliance.

NOTES:

- Amazon S3 Access Points, which are network endpoints used to manage access to shared data in Amazon S3 Buckets, are supported for use with the *Object Lock* feature.
- This Compliance Assessment Report **excludes**:
  - *Express One Zone* S3 directory Bucket types, which do not support the use of *Object Lock*.
  - S3 Outposts (i.e., customers running their own on-premises implementation of S3).
  - Amazon S3 in a dedicated cloud not hosted by Amazon.
  - Software-as-a-Service solutions not managed by Amazon, which store objects in S3 but do not utilize the S3 *Object Lock* features.

2 • Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e)

This section presents Cohasset's assessment of the functionality of Amazon S3, for compliance with the electronic recordkeeping system requirements promulgated in SEC Rules 17a-4(f)(2) and 18a-6(e)(2), as well as describes how the solution supports the regulated entity in meeting the audit system requirement of SEC Rules 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii).

For each compliance requirement described in this section, this assessment is organized as follows:

- ***Compliance Requirement*** – Excerpt of relevant regulatory requirement in SEC Rules 17a-4(f) and 18a-6(e) and Cohasset's interpretation of the specific requirement
  - Both SEC Rules 17a-4(f) and 18a-6(e) are addressed in this section, since the electronic recordkeeping system requirements (principles, controls and testable outcomes) are the same, though the Rules specify their respective regulations and regulators and include semantic differences.
- ***Compliance Assessment*** – Summary statement assessing compliance of Amazon S3
- ***Amazon S3 Capabilities*** – Description of assessed functionality
- ***Additional Considerations*** – Additional clarification related to meeting the specific requirement

The following sections document Cohasset's assessment of the capabilities of Amazon S3, as described in Section 1.3, *Amazon S3 Overview and Assessment Scope*, relative to the enumerated requirements of SEC Rules 17a-4(f) and 18a-6(e).

2.1 Record and Audit-Trail

2.1.1 Compliance Requirement

This regulatory requirement, adopted with the 2022 Rule amendments, allows regulated entities to use a combination of electronic recordkeeping systems, with each system meeting either (a) the record and audit-trail requirement, as described in this section or (b) the non-rewriteable, non-erasable record format requirement, as explained in Section 2.2, *Non-Rewriteable, Non-Erasable Record Format*.

This record and audit-trail requirement is designed to permit use of the regulated entities' business-purpose recordkeeping systems to achieve the required outcome without specifying any particular technology solution.

SEC 17a-4(f)(2)(i)(A) and 18a-6(e)(2)(i)(A):

Preserve a record for the duration of its applicable retention period in a manner that maintains a complete time-stamped audit-trail that includes:

(1) All modifications to and deletions of the record or any part thereof;

(2) The date and time of actions that create, modify, or delete the record;

(3) If applicable, the identity of the individual creating, modifying, or deleting the record; and

(4) Any other information needed to maintain an audit-trail of the record in a way that maintains security, signatures, and data to ensure the authenticity and reliability of the record and will permit re-creation of the original record if it is modified or deleted

The SEC clarifies that this requirement to retain the record and its complete time-stamped audit-trail promotes the authenticity and reliability of the records by requiring the electronic recordkeeping system to achieve the testable outcome of reproducing the original record, even if it is modified or deleted during the required retention period, without prescribing how the system meets this requirement.

> *[L]ike the existing WORM requirement, [the audit-trail requirement] sets forth a specific and testable outcome that the electronic recordkeeping system must achieve: the ability to access and produce modified or deleted records in their original form.*[5] [emphasis added]

For clarity, the record and audit-trail requirement applies only to the final records required by regulation.

> *[T]he audit-trail requirement applies to the final records required pursuant to the rules, rather than to drafts or iterations of records that would not otherwise be required to be maintained and preserved under Rules 17a-3 and 17a-4 or Rules 18a-5 and 18a-6.*[6] [emphasis added]

2.1.2 Compliance Assessment

In this report, Cohasset has not assessed Amazon S3 in comparison to this requirement of the SEC Rules.

For enhanced control, a business-purpose recordkeeping system may store records and complete time-stamped audit-trails on Amazon S3, with the features and controls described in Sections 2.2 through 2.6 of this report.

Reminder: This requirement pertains to the regulated entity's business-purpose data processing system (i.e., a trading system), when configured to retain the record and its complete time-stamped audit trail. This requirement is an alternative to the more stringent non-rewriteable, non-erasable record format requirement (i.e., write-once, read-many or WORM requirement), which is assessed in Section 2.2.

2.2 Non-Rewriteable, Non-Erasable Record Format

2.2.1 Compliance Requirement

SEC 17a-4(f)(2)(i)(B) and 18a-6(e)(2)(i)(B):
Preserve the records exclusively in a non-rewriteable, non-erasable format

This regulatory requirement was first adopted in 1997. In the 2022 Rule amendments, regulated entities are allowed to use a combination of electronic recordkeeping systems, to comply with each system meeting either (a) the non-rewriteable, non-erasable record format requirement described in this section or (b) the complete time-stamped record audit-trail requirement described in Section 2.1, *Record and Audit-Trail*.

The SEC further clarifies that the previously issued interpretations are extant. Therefore, records must be preserved in a non-rewriteable, non-erasable format that prevents overwriting, erasing, or otherwise altering records during the required retention period, which may be accomplished by any combination of hardware and software integrated controls.

> *The 2003 interpretation clarified that the WORM requirement does not mandate the use of optical disks and, therefore, a broker-dealer can use "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." The*

5 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.

6 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66418.

> *2019 interpretation further refined the 2003 interpretation. In particular, it noted that the 2003 interpretation described a process of integrated software and hardware codes and clarified that "a software solution that prevents the overwriting, erasing, or otherwise altering of a record during its required retention period would meet the requirements of the rule."*
> *****
> *In 2001, the Commission issued guidance that Rule 17a-4(f) was consistent with the ESIGN Act. The final amendments to Rule 17a-4(f) do not alter the rule in a way that would change this guidance.*[7] [emphasis added]

Moreover, records must be preserved beyond established retention periods when certain circumstances occur, such as a subpoena or legal hold:

> *[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.*[8] [emphasis added]

2.2.2 Compliance Assessment

It is Cohasset's opinion that the functionality of Amazon S3, with *Object Lock* retention controls applied to records in either highly restrictive *Compliance* mode or less-restrictive *Governance* mode, meets this SEC requirement to retain records in non-rewriteable, non-erasable format for the applied time-based[9] retention periods and legal holds, when (a) properly configured, as described in Section 2.2.3 and (b) the considerations described in Section 2.2.4 are satisfied.

Reminder: This non-rewriteable, non-erasable record format requirement is a more stringent alternative to the complete time-stamped audit-trail requirement, which is addressed in Section 2.1.

2.2.3 Amazon S3 Capabilities

This section describes the functionality of Amazon S3 that directly pertains to this SEC requirement to preserve electronic books and records in a non-rewriteable, non-erasable format, for the required retention period and any applied legal holds.

2.2.3.1 Overview

- Objects (e.g., data, images and files), together with associated metadata, are transmitted to Amazon S3 and stored in Buckets.
- To meet the requirements of SEC Rules 17a-4(f) and 18a-6(e):
  - Each new or existing Bucket intended to store required records must have both: (a) the Amazon S3 *Object Lock* feature enabled (On) and (b) versioning enabled, to allow each object version to be retained as a separate record with its own retention and legal hold controls.

---

7 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66419.

8 Electronic Storage of Broker-Dealer Records, Exchange Act Release No. 47806 (May 7, 2003), 68 FR 25283, (May 12, 2003) (2003 Interpretative Release).

9 Time-based retention periods require records to be retained for a fixed contiguous period of time from the creation or storage timestamp.

- Retention controls (i.e., the *Object Lock* mode of highly-restrictive *Compliance* or less restrictive *Governance* mode and *Retain Until Date)* must be applied and stored as metadata for each object version that is a required record.
- Optionally, the *Legal Hold* status for an object version may be enabled (On), as needed, to suspend eligibility for deletion until the *Legal Hold* status is disabled (Off).

► The following table summarizes the *Object Lock* controls applied in either *Compliance* or *Governance* mode. See the subsections following this *Overview*, for information on configuring the retention features and the resulting integrated controls.

	***Object Lock*, in highly-restrictive *Compliance* mode**	***Object Lock*, in less-restrictive *Governance* mode**
Protecting record content and immutable metadata	• By design, each record version and its immutable metadata cannot be modified for its lifespan. • The versioning feature, which is required when using *Object Lock*, ensures that objects are not modified or overwritten; instead, a new version is created, with separate retention controls. • Renaming Buckets, objects, and version identifiers is prohibited.	
Restricting changes to applied retention controls	• The *Object Lock* feature applied to a Bucket cannot be removed. • For record versions set to *Compliance* mode, authorized users and/or lifecycle policies: ○ Cannot downgrade the *Object Lock* mode to *Governance* or remove the *Object Lock* mode. ○ Cannot reduce the *Retain Until Date,* however, the date may be extended, as needed. Accordingly, *Compliance* mode assures that *Object Lock* retention controls are not circumvented by any user or process. • See Section 2.2.3.3, *Record Definition and Retention Controls.*	• The *Object Lock* feature applied to a Bucket cannot be removed. • For record versions set to *Governance* mode, administrators with ***BypassGovernanceRetention*** permissions: ○ Can change *Governance* mode to *Compliance* or remove the *Object Lock* mode entirely. ○ Can extend, reduce or remove the *Retain Until Date.* Accordingly, procedural controls and monitoring are required to scrutinize privileged administrator actions taken to modify or remove *Object Lock* retention controls. • See Section 2.2.3.3, *Record Definition and Retention Controls*.
Applying and removing legal holds	• A *Legal Hold* attribute may be enabled (On) which prevents deletion of that object version until the *Legal Hold* attribute is disabled (Off). See Section 2.2.3.4, *Legal Holds (Temporary Holds).*	
Restricting deletion of records and Buckets	• Deleting a record version is allowed only when both the *Retain Until Date* is expired and the *Legal Hold* attribute is disabled (Off).	• Administrators with ***BypassGovernanceRetention*** permissions may delete unexpired object versions. Therefore, procedural controls and monitoring are required to scrutinize privileged administrator actions to prematurely delete record versions.
	• Deleting a record (without identifying the Version) appends a delete marker as the current (top) version. • A Bucket cannot be deleted unless it is empty. • See Section 2.2.3.5, *Deletion Controls.*	

► The features and protections listed above apply across all Amazon S3 storage classes, including Amazon Glacier[10] (archival storage). Therefore, lifecycle policies may be used to tier protected objects in Amazon S3 storage classes.

[10] The Amazon S3 *Object Lock* feature is in addition to the previously released Amazon Glacier *Vault Lock* feature for preserving record objects in a non-rewriteable and non-erasable format.

2.2.3.2 Amazon S3 Retention-related Configurations

- The following table describes S3 Bucket, Identity and Access Management (IAM), and Lifecycle configurations related to the S3 *Object Lock* feature. See Section 2.2.3.3, *Record Definition and Retention Controls*, for details on the resulting integrated controls applied to records.

	Bucket, IAM Policy and Lifecycle Policy Configurations related to S3 *Object Lock*
Bucket Name	• The Bucket name must be globally unique across Amazon S3.
Enabling the *Object Lock* feature	• For each new or existing Bucket intended to retain required records, the *Object Lock* **feature** must be enabled (On). Once enabled for a Bucket, this configuration cannot be suspended or disabled.

Versioning	• Versioning must be enabled on the Bucket in advance of enabling the *Object Lock* feature. Once both are enabled, versioning cannot be suspended or disabled.
	  ○ New object versions are created with write requests such as (a) write a new object version, (b) update user-defined metadata (i.e., name-value pairs) and (c) copy an object.
	  ○ New object versions are not created when modifying retention, legal hold controls, or changing the *Object Lock* mode from *Governance* to *Compliance* for an object version. Additionally, modifications to Amazon S3 access control lists (ACLs) and Amazon S3 tags do not result in storing a new object version.
	• Each object version is separately managed, with separate retention and legal hold controls. When controls are set without specifying a version, the controls apply to the current (top) version.

Default Retention Period and Object Lock	• Optionally, a pair of Bucket defaults may be configured to automatically apply retention controls to each object version being stored, unless retention controls are explicitly transmitted with the object version.
	  ○ The **Default *Object Lock* mode** is set to either *Compliance* (highly-restrictive) or *Governance* (less restrictive).
	  ○ The **Default retention period** (i.e., specified in terms of days or years, between 1 day and 100 years) is added to the creation/storage timestamp to calculate the object version's *Retain Until Date*.
	See section 2.2.3.3, *Record Definition and Retention Controls*, for more information, including details on the retention controls associated with each mode.
	• Authorized users may change the Bucket default values at any time, including: (a) shortening the *Default retention period*, (b) changing the default *Object Lock* mode between *Governance* and *Compliance,* or (c) clearing (removing) both default values. The updated default values apply day-forward and do not apply to previously stored object versions; therefore, protections (if any) previously applied to an object version remain unchanged.
	• Note: Setting these defaults assures retention controls are applied to all new object versions in the Bucket.

Bucket Minimum and Maximum Retention Periods	• Optionally, Minimum and Maximum retention periods (Min/Max range) may be configured for the Bucket. When an object is transmitted, if the *Retain Until Date* is outside the Min/Max range configured for the Bucket, the object will be rejected, and an error will be reported.
	  ○ The Bucket Default retention period must be set between the Min/Max range to ensure that objects using the Bucket Default are not rejected during write.
	  ○ When the Min/Max range is set for a Bucket, all users of the Bucket are bound by the same Min/Max range.
	• Authorized users may change the Min/Max range at any time. The updated Min/Max range applies day-forward and does not apply to previously stored objects.
	• Both Bucket and IAM Min/Max retention values (see next row) are honored when retention is applied or updated for an object version.

IAM Policies	• Optionally, Minimum and Maximum retention periods (Min/Max range) may be configured, using conditional operators for Identity and Access Management (IAM) roles. For example, an IAM Role is defined and permissioned to apply retention periods between [Minimum] and [Maximum] period. The IAM Role is applied to users (e.g., source systems) permissioned to store objects in the Bucket.

	Bucket, IAM Policy and Lifecycle Policy Configurations related to S3 *Object Lock*
	○ When the Min/Max range is set through IAM, each permissioned user of a Bucket may be bound by a different Min/Max range. ● Authorized users may change the Min/Max range for an IAM role at any time. The updated Min/Max range applies day-forward and does not apply to previously stored objects. ● Both Bucket and IAM Min/Max retention values are honored when retention is applied or updated for an object version.
Lifecycle Policies	● Optionally, lifecycle policies may be configured for a Bucket to set rules to (a) transition objects to tiered (cold) storage or (b) perform *expiration* and *deletion* actions, which may append a delete marker or permanently delete an object version. ● When more than one lifecycle policy applies to a Bucket, permanent deletion of eligible object versions takes precedence over transitioning to tiered storage. ● Lifecycle policies apply to all new and existing objects stored in the Bucket.

2.2.3.3 Record Definition and Retention Controls

- Each object version is managed as a separate record, with an explicit *Retain Until Date* and *Object Lock* mode. Each record (i.e., object version) is comprised of:
  - The complete content of the object, which is unmodifiable.
  - Immutable metadata, which includes, but is not limited to, unique Object Key Name, version identifier, creation/storage timestamp (*lastmodified* attribute), object size, and user-defined metadata (name-value pairs).
  - Mutable metadata, which includes, but is not limited to, retention controls (*Retain Until Date* and *Object Lock* mode), Amazon S3 access control lists (ACLs), and Amazon S3 tags.
- The following table summarizes the retention metadata applied to the object during the initial storage process, based on (a) explicit retention attributes **transmitted as a pair** with the object version (column with orange highlighted headings) and (b) the Bucket's default retention settings (columns with blue highlighted headings).

Transmitted *Object Lock* Mode	**Transmitted *Retain Until Date***	**Object version's retention attributes, when the Bucket has no default retention settings**	**Object version's retention attributes, when the Bucket has default retention settings**
Null	MM/DD/YYYY	● Error returned, write operation fails because both retention attributes were not transmitted.	
Null	Null	● Object version is stored without retention controls.	● Object version is set to the default retention mode and the *Retain Until Date* is calculated by adding the Bucket's Default retention period to the object version's creation/storage timestamp.
Governance	MM/DD/YYYY	● If the transmitted *Retain Until Date* falls within the allowable Min/Max range, the object version is set to *Governance* mode and *Retain Until Date* is MM/DD/YYYY. ● If the transmitted *Retain Until Date* falls outside the allowable Min/Max range, an error is returned and the write operation fails.	
Governance	Null	● Error returned, write operation fails because both retention attributes were not transmitted.	

Transmitted *Object Lock* Mode	Transmitted *Retain Until Date*	Object version's retention attributes, when the Bucket has no default retention settings	Object version's retention attributes, when the Bucket has default retention settings
Compliance	MM/DD/YYYY	• If the transmitted *Retain Until Date* falls within the allowable Min/Max range, the object version is set to *Compliance* mode and *Retain Until Date* is MM/DD/YYYY. • If the transmitted *Retain Until Date* falls outside the allowable Min/Max range, an error is returned and the write operation fails.	
Compliance	Null	• Error returned, write operation fails because both retention attributes were not transmitted.	

- For large objects transmitted using Amazon S3 multipart upload capabilities, the creation/storage timestamp is captured at the start of the upload process. This timestamp is used to calculate a *Retain Until Date* for the object, when an explicit *Retain Until Date* is not transmitted with the object. *Object Lock* controls are applied when the entire multi-part upload is complete and verified.
- In addition to applying retention controls during record creation/storage, explicit retention controls may be applied to existing object versions, as described in the following table. In all cases:
  - The *Object Lock* mode and *Retain Until Date* must be set as a pair; therefore, only pairs are depicted in the table.
  - The new *Retain Until Date* must fall within the current allowable Min/Max range or an error is returned and the update fails.
  - Retention controls are applied to the explicit version if the version identifier is specified, otherwise, the controls are applied to the current (top) version.

Current *Object Lock* Mode	Transmitted *Object Lock* Mode	Transmitted *Retain Until Date*	Modifications to the object version's retention attributes
Null	Governance	MM/DD/YYYY	• Object version is set to *Governance* mode and *Retain Until Date* is MM/DD/YYYY.
Null	Compliance	MM/DD/YYYY	• Object version is set to *Compliance* mode and *Retain Until Date* is MM/DD/YYYY.
Governance	Null	Null	• Retention controls are removed only if the administrator (a) has *BypassGovernanceRetention* permission and (b) explicitly specifies the "bypass-governance-retention" header in the request; otherwise, an error is returned, and the operation fails.
Governance	Governance	MM/DD/YYYY	• If the *Retain Until Date* is being extended, the operation succeeds. • If the *Retain Until Date* is being reduced, the operation succeeds only if the administrator has *BypassGovernanceRetention* permissions.
Governance	Compliance	MM/DD/YYYY	• If the *Retain Until Date* matches the current setting or is being extended, the operation succeeds. • If the *Retain Until Date* is being reduced, the operation succeeds only if the administrator (a) has *BypassGovernanceRetention* permission and (b) explicitly specifies the "bypass-governance-retention" header in the request; otherwise, an error is returned, and the operation fails.

Current *Object Lock* Mode	Transmitted *Object Lock* Mode	Transmitted *Retain Until Date*	Modifications to the object version's retention attributes
Compliance	Null	Null	• Operation fails because *Compliance* mode retention controls cannot be removed by any user, even administrators with the *BypassGovernanceRetention* permission.
Compliance	Governance	MM/DD/YYYY	• Operation fails because *Compliance* mode retention controls cannot be changed to the less-restrictive *Governance* mode by any user, even administrators with the *BypassGovernanceRetention* permission.
Compliance	Compliance	MM/DD/YYYY	• If the *Retain Until Date* is being extended, the operation succeeds. • If the *Retain Until Date* is being reduced, the operation fails because *Compliance* mode retention controls cannot be made less restrictive (cannot be reduced).

- Amazon S3 Batch Operations provide the ability to apply or update *Object Lock* retention controls to many objects with a single request. Batch Operations require that:
  - Versioning and S3 *Object Lock* are enabled on the specified Bucket.
  - All target objects must be retained within the same Bucket.

  The Batch Operation job runs until completion or until an operation fails, based upon the rules defined in the preceding table.
- An assortment of retention controls is allowed within a single Bucket. For example, a Bucket with the *Object Lock* feature enabled, but with no default values, may contain object versions (a) locked with *Compliance* mode, (b) locked with *Governance* mode, or (c) unprotected. Additionally, the *Legal Hold* attribute may be applied to object versions, independent of retention controls.
- When *Object Lock* is applied to objects, integrated controls protect the records from certain actions. The following table describes the integrated retention controls applied to each record with *Object Lock* in *Compliance* and *Governance* modes.

	***Object Lock*, in highly-restrictive *Compliance* mode**	***Object Lock*, in less-restrictive *Governance* mode**
Managing versions, and protecting record content and immutable metadata	• Versioning must be enabled on the Bucket. When enabled, each version of an object is considered a separate record and must have its own applied *Object Lock* mode, *Retain Until Date*, and *Legal Hold* attribute (optional). • Each version, together with its *immutable attributes* (metadata), is immutably stored for its lifespan. ○ All attempts to **modify** the contents of a version, during its lifespan, are rejected. ○ All attempts to **overwrite** an existing record result in storing a new version with separately applied retention controls and *Legal Hold* attribute (if applicable) ○ All attempts to change the unique Object Key Name are rejected. Additionally, version identifiers are system-generated and are immutable. ○ If an object is uploaded with an Object Key Name that already exists in the Bucket, a new version, with a new version identifier is automatically created. ○ If user-defined custom metadata (name-value pairs) are added or modified for a record, a new version is automatically created. ○ If the *Object Lock* mode, *Retain Until Date*, *Legal Hold* attribute, ACLs, or Amazon S3 tags are added or modified for a record, updates are stored without creating a new version. • After retention controls expire and any *Legal Hold* is disabled (Off), the version may be deleted but cannot be modified or overwritten.	

	***Object Lock*, in highly-restrictive *Compliance* mode**	***Object Lock*, in less-restrictive *Governance* mode**
Modifying or removing retention controls	● For records set to *Compliance* mode, authorized users and/or lifecycle policies: ○ Cannot change the *Object Lock* mode to *Governance* or remove the *Object Lock* mode. ○ Cannot reduce the *Retain Until Date,* however, the date may be extended as needed. Accordingly, *Compliance* mode assures that *Object Lock* retention controls are not circumvented by any user or process.	● For records set to *Governance* mode, administrators with ***BypassGovernanceRetention*** permissions: ○ Can change *Governance* mode to *Compliance* or remove the *Object Lock* mode entirely. ○ Can extend, reduce or remove the *Retain Until Date.* Accordingly, procedural controls and monitoring are required to scrutinize privileged administrator actions taken to modify or remove *Object Lock* retention controls.
Applying and removing legal holds	● A *Legal Hold* attribute may be enabled (On) which prevents the overwrite or deletion of that object version until the *Legal Hold* attribute is disabled (Off). ○ The *Legal Hold* attribute may be enabled regardless of an object version's *Object Lock* status. ○ Bypassing *Governance* mode controls does not affect an object's legal hold status; if an object version's *Legal Hold* attribute is enabled (On), attempts to delete the object version are prohibited. ● See Section 2.2.3.4, *Legal Holds (Temporary Holds).*	
Restricting deletion of records and Buckets	● Deleting a record version is allowed only when both the *Retain Until Date* is expired and the *Legal Hold* attribute is disabled (Off).	● Administrators with ***BypassGovernanceRetention*** permission may delete unexpired object versions. Therefore, procedural controls and monitoring are required to scrutinize privileged administrator actions to prematurely delete record versions.
	● Deletion of the record (without identifying the version) appends a delete marker as the current (top) version and all other existing record versions are hidden but remain unmodifiable. The Delete marker may be removed to reinstate the original record versions. ● A Bucket cannot be deleted unless it is empty. ● See Section 2.2.3.5, *Deletion Controls.*	
Copying records	● An object may be copied between Amazon S3 Buckets, resulting in the creation of a new copy with its own unique metadata, which may include the assignment of a *Retain Until Date*, *Object Lock* mode and *Legal Hold* status. The original record and its metadata will remain, unaltered, in the source Bucket.	
Moving records	● An object cannot be moved between Amazon S3 Buckets, unless the object is eligible for deletion. If the object is eligible for deletion, the move results in deleting the expired object from the source Bucket and creating a new, unprotected object in the target Bucket.	
Changing permissions	● Access control lists (ACLs) may be modified, by authorized users, at any time.	

2.2.3.4 Legal Holds (Temporary Holds)

When a record is subject to preservation requirements for subpoena, litigation, regulatory investigation or other special circumstances, it must be preserved immutably, (i.e., any deletion, modification or overwrite must be prohibited) until the hold is removed.

- The *Legal Hold* (On/Off) status may be applied to any object version stored in a Bucket with the Amazon S3 *Object Lock* feature enabled (On).
  - Each object version includes a separate *Legal Hold* status attribute. When the *Legal Hold* status is enabled (On), it prohibits deleting the object version, and when disabled (Off), it no longer mandates preservation of the object version; however other retention controls continue to apply.

- The *Legal Hold* status is independent of the object's *Retain Until Date* and *Object Lock* mode; therefore, a *Legal Hold* status may be applied to an object without an applied *Retain Until Date* and *Object Lock* mode.
- Bypassing *Governance* mode controls does not circumvent an object's *Legal Hold* status; if an object version's *Legal Hold* attribute is enabled (On), attempts to delete the object version are prohibited.

2.2.3.5 Deletion Controls

- An object version, together with its metadata, is eligible for deletion when (a) its *Retain Until Date* has expired (is in the past) and (b) its *Legal Hold* attribute is disabled (Off).
  - Eligibility for deletion does not cause automatic deletion.
- The following table summarizes actions taken to delete record versions and manage delete markers.

	Deletion when *Object Lock* is applied in highly-restrictive *Compliance* mode	**Deletion when *Object Lock* is applied in less restrictive *Governance* mode**

Deleting records (without specifying the version identifier)	• When deleting an object without also specifying the version identifier, a delete marker is added as the current (top) version, whether or not the object is eligible for deletion.
	  ○ The delete marker does not affect the stored versions of the object.
	• Delete markers can be removed, which results in reinstating or recovering the deleted (hidden) object versions.
	• A Lifecycle Policy may be configured to issue delete requests without specifying a version identifier:
	  ○ If the current version is not a delete marker, Amazon S3 adds a delete marker with a unique version identifier and makes the delete marker the current version.
	  ○ If the current version is a delete marker and one or more older versions also exist, no action is taken by the lifecycle policy.
	  ○ If the current version is a delete marker and it is the only version (i.e., an expired object delete marker), Amazon S3 permanently deletes the delete marker.
	• Note: See Section 2.4, *Capacity to Download and Transfer Records and Location Information*, for information on the implications of delete markers on search and retrieval.	

Deleting records (when the version identifier is specified)	• When deleting an object version (i.e., when specifying the version identifier), *Object Lock* protections apply, and only eligible versions are deleted. ○ An error is logged, and the action is rejected if the user does not have the required permissions or the user attempts to delete an object version when (a) the *Retain Until Date* has not passed or (b) the *Legal Hold* status is set (On). • A Lifecycle Policy may be configured to automatically delete object versions. Only object versions that are eligible for deletion will be permanently deleted.	
	• Privileged delete (i.e., *BypassGovernanceRetention*) is not available to any administrator or user to prematurely delete object versions.	• Administrators with *BypassGovernanceRetention* permission may delete unexpired object versions; however, the *BypassGovernanceRetention* override cannot be utilized with a Lifecycle Policy. • Accordingly, procedural controls and monitoring are required to scrutinize privileged administrator actions and ensure compliant retention protections are not circumvented.
Deleting Buckets	• A Bucket with the *Object Lock* feature enabled cannot be deleted until the Bucket is empty. Accordingly, deleting a Bucket to effectuate the premature deletion of records is prohibited.	

2.2.3.6 Security

- Amazon Web Services are designed to meet Enterprise security and compliance requirements.
- Objects and metadata are encrypted:
  - Optionally, data in-transit (data traveling to and from Amazon S3) may be protected using Secure Sockets Layer/Transport Layer Security (SSL/TLS) or by client-side encryption.
  - Amazon S3 offers options for protecting data at rest (data stored on disks in Amazon S3 data centers):
    - **Server-Side Encryption** – By default, Amazon S3 encrypts objects with **Amazon S3-Managed Keys (SSE-S3)** before each is stored in its data centers and decrypts each object it when downloaded. SS3-S3 encryption ensures that each object is encrypted with a unique key employing strong multi-factor encryption. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates.
    - To use a different type of server-side encryption, one of the following options may be specified in the PUT command or set as the default configuration for the destination Bucket.
      - **Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)** – This feature is similar to SSE-S3, with added protection against unauthorized access of objects in S3 and an audit trail showing when the key was used and by whom. Additionally, encryption keys may be created and managed by the client.
      - **Dual-layer Server-Side Encryption with AWS KMS keys (DSSE-KMS)** – this feature is similar to SSE-KMS, except it applies **two** individual layers of encryption to objects instead of one. DSSE-KMS fulfills compliance standards that require multilayer encryption, while still maintaining the ability to access and analyze stored data by a variety of AWS services and tools.
      - **Server-Side Encryption with Customer-Provided Keys (SSE-C)** – The client manages the encryption keys and Amazon S3 manages the encryption, as it writes to disks, and decryption, when objects are accessed.
    - **Client-Side Encryption** – The regulated entity may encrypt data before uploading it to Amazon S3 for storage. With this option, the regulated entity manages the encryption process, the encryption keys, and related tools.
  - Roles-Based Security (RBAC) is employed by AWS. The permissions for each user are controlled through IAM roles created for the client organization.

2.2.3.7 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 S3 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 on Amazon S3. These controls prevent or correct any inadvertent or intentional administrative modifications of the time clock, which could allow for premature deletion of objects.

2.2.4 Additional Considerations

In addition, for this non-rewriteable, non-erasable record format requirement, the regulated entity is responsible for:

- Configuring Buckets intended to store required records with the *Object Lock* feature. Cohasset recommends configuring a *Default Object Lock* mode of *Compliance* or *Governance* and an appropriate *Default retention period* to assure all records are stored with integrated retention controls.
- Optionally, the regulated entity may set *Minimum and Maximum retention periods* to validate the *Retain Until Date* applied to each object.
- Ensuring all records required for compliance with the Rules are successfully stored with appropriate retention controls, preferably within 24 hours of creation.
- Storing records requiring event-based[11] retention in a separate compliance system or otherwise planning for event-based retention, since Amazon S3 does not currently support event-based retention.
- Establishing and implementing procedures to monitor and scrutinize privileged administrative activities if *Object Lock* is set to less-restrictive *Governance* mode. For example, implement separation of duties for administrators, require management approval prior to removing or reducing retention, and regularly monitor privileged administrative actions.
- Limiting the creation and management of delete markers. Specifically, Cohasset recommends always specifying the version identifier in delete requests.
- Setting a *Legal Hold* status to On or otherwise protecting records that require preservation for legal matters, government investigations, external audits and other similar circumstances, and setting the *Legal Hold* status to Off, when preservation is no longer required.
- Appropriately assigning permissions required to manage the retention controls and properly configuring the Identity and Access Management (IAM) roles.

Additionally, the regulated entity is responsible for (a) maintaining its AWS Management Account in good standing, paying for appropriate services, and procedurally prohibiting administrators from closing its Management Account or Member Accounts[12] until the applied retention periods and holds have expired for all retained records or until the records have been transferred to another compliant storage system, (b) authorizing user privileges, and (c) maintaining appropriate technology, encryption keys, and other information and services needed to access the records.

[11] Event-based retention periods require records to be retained indefinitely until a specified condition is met (e.g., a contract expires or an employee terminates), after which the record is retained for a fixed final retention period.

[12] Similar to decommissioning infrastructure, closing a Management Account or a Member Account will delete the associated Amazon S3 Buckets and retained objects, even if the objects are not eligible for deletion.

2.3 Record Storage Verification

2.3.1 Compliance Requirement

SEC 17a-4(f)(2)(ii) and 18a-6(e)(2)(ii):
Verify automatically the completeness and accuracy of the processes for storing and retaining records electronically

The electronic recordkeeping system must automatically verify the completeness and accuracy of the processes for storing and retaining records electronically, to ensure that records read from the system are precisely the same as those that were captured.

This requirement includes both quality verification of the recording processes for storing records and post-recording verification processes for retaining complete and accurate records.

2.3.2 Compliance Assessment

Cohasset affirms that the functionality of Amazon S3 meets this SEC requirement for complete and accurate recording of records and post-recording verification processes, when the considerations identified in Section 2.3.4 are satisfied.

2.3.3 Amazon S3 Capabilities

The recording and post-recording verification processes of Amazon S3 are described below.

2.3.3.1 Recording Process

- A checksum must be transmitted with any object to be stored in a Bucket with the *Object Lock* feature enabled. The object will be stored only if the checksum value calculated by Amazon S3 matches the uploaded checksum. If it does not match, an error is reported, and the object must be re-uploaded.
- Large objects, greater than 100MB in size, may be transmitted using Amazon's multipart upload capabilities, The object is divided into contiguous parts which can be transmitted in any order for storage in an Amazon S3 Bucket. Checksums are transmitted with each part of the object and used to validate each upload. Once all parts are successfully uploaded, Amazon S3 assembles them to create the object and a checksum for the complete object is saved as metadata.
- Amazon S3 utilizes advanced electronic recording technology which applies a combination of checks and balances to ensure that objects are written in a high quality and accurate manner.

2.3.3.2 Post-Recording Verification Process

- Standard Amazon S3 storage is designed to provide 99.999999999% (11-nines) durability and 99.99% availability of objects over a given year.
- Amazon S3 regularly verifies the integrity of data stored using checksums. If Amazon S3 detects data corruption, it is repaired using redundant data.
- Amazon S3 also calculates checksums on all network traffic to detect corruption of data packets when storing or retrieving data.

2.3.4 Additional Considerations

- The source system is responsible for transmitting the complete contents of the required records, with a checksum, and Amazon S3 validates the accuracy of the recording process.
- For retrieval, Cohasset recommends that the source system request the checksum for the object and use it to validate transmission of the downloaded object.

2.4 Capacity to Download and Transfer Records and Location Information

2.4.1 Compliance Requirement

SEC 17a-4(f)(2)(iv) and 18a-6(e)(2)(iv):
Have the capacity to readily download and transfer copies of a record and its audit-trail (if applicable) in both a human readable format and in a reasonably usable electronic format and to readily download and transfer the information needed to locate the electronic record, as required by the staffs of the Commission, [and other pertinent regulators] having jurisdiction over the [regulated entity]

This requirement calls for an adequate capacity to readily download records and information needed to locate the record in both a:

- Human readable format that can be naturally read by an individual, and
- Reasonably usable electronic format that is compatible with commonly used systems for accessing and reading electronic records.

The downloaded records and information needed to locate the records (e.g., unique identifier, index, or properties) must be transferred to the regulator, in an acceptable format.

Further, this requirement to download and transfer the complete time-stamped audit-trail applies only when this alternative is utilized; see Section 2.1, *Record and Audit-Trail*.

2.4.2 Compliance Assessment

Cohasset asserts that the functionality of Amazon S3 meets this SEC requirement to maintain the capacity to readily download and transfer the records and information used to locate the records, when the considerations described in Section 2.4.4 are satisfied.

2.4.3 Amazon S3 Capabilities

The following capabilities relate to the capacity to readily search, access, download, and transfer records and the information needed to locate the records.

- Each record in Amazon S3 is assigned a unique identifier, which facilitates findability. Specifically, Amazon S3 captures the following metadata for each record version and immutably retains this metadata for the lifespan of the record.
  - A unique ***Object Key Name*** which is comprised of the Bucket name, prefix and object name. Note: the Bucket name must be globally unique across Amazon S3, and the object name must be unique within the Bucket.
  - A ***version identifier***, which is automatically assigned to each new version of the object.
  - The creation/storage timestamp, which is system-generated.

- Amazon assures that AWS hardware and software capacity allows for ready access to the records and metadata. Further, Amazon maintains redundant storage media, network, and power to mitigate outages that would result in unavailability of data. Standard Amazon S3 storage is designed to provide 99.999999999% (11-nines) durability and 99.99% availability of objects over a given year.
- Using the Amazon S3 API, Command Line Interface (CLI) or Management Console, authorized users can:
  - Use the S3 Console and click the version switch to see retention controls for each object version.
  - Run an inventory report for a specific Bucket and list records in lexicographic order.
  - List records in a Bucket (selection criteria may be defined to find and return a subset of the objects in a Bucket) using the following command:
    - **ListObjects** and **ListObjectsV2**: Returns a list of the objects, by S3 Object Key; if the most recent version is a delete marker the object is not returned in the list.
    - **ListObjectVersions**: Returns metadata for all versions of the objects in a Bucket, sorted by S3 Object Key, along with all versions associated with each. If a delete marker is the most recent version of the object, the criteria must be specified in the search.
    - **HeadObject**: Returns the object metadata, including retention settings for the current (top) version, without returning the object itself.
  - Get objects using the **GetObject** command:
    - When the request includes the version identifier, the specific object version is returned.
    - When no version identifier is specified, the most recent version is returned, unless the most recent version is a delete marker, in which case an error code is returned.
  - Download selected objects and associated metadata to a designated storage location. When multiple versions of a record are stored, the top-level version is returned, by default. The specific version identifier must be specified in the search and download requests.

  For each of the above actions, based on user permissions, certain metadata will be returned, including Object Key Name, version identifier, creation/storage timestamp, *Retain Until* date, *Object Lock* mode, and *Legal Hold* status for each object.

2.4.4 Additional Considerations

In addition, for this requirement, the regulated entity is responsible for: (a) maintaining its account in good standing, (b) authorizing user privileges, (c) maintaining appropriate technology and resource capacity, encryption keys, and other information and services needed to use Amazon S3 to readily access, download, and transfer the records and the information needed to locate the records, and (d) providing requested information to the regulator in the requested format.

2.5 Record Redundancy

2.5.1 Compliance Requirement

SEC 17a-4(f)(2)(v) and 18a-6(e)(2)(v):

(A) Include a backup electronic recordkeeping system that meets the other requirements of this paragraph [(f) or (e)] and that retains the records required to be maintained and preserved pursuant to [§ 240.17a-3 or § 240.18a-5] and in accordance with this section in a manner that will serve as a redundant set of records if the original electronic recordkeeping system is temporarily or permanently inaccessible; or

(B) Have other redundancy capabilities that are designed to ensure access to the records required to be maintained and preserved pursuant to [§ 240.17a-3 or § 240.18a-5] and this section

The intent of this requirement is to retain a persistent alternate source to reestablish an accessible, complete and accurate record, should the original electronic recordkeeping system be temporarily or permanently inaccessible.

The 2022 final Rule amendments promulgate two redundancy options, paragraphs (A) or (B).

- The intent of paragraph (A) is:

  [B]ackup electronic recordkeeping system must serve as a redundant set of records if the original electronic recordkeeping system is temporarily or permanently inaccessible because, for example, it is impacted by a natural disaster or a power outage.[13] [emphasis added]

- The intent of paragraph (B) is:

  [R]edundancy capabilities that are designed to ensure access to Broker-Dealer Regulatory Records or the SBS Entity Regulatory Records must have a level of redundancy that is at least equal to the level that is achieved through using a backup recordkeeping system.[14] [emphasis added]

Note: The alternate source must meet *"the other requirements of this paragraph [(f)(2) or (e)(2)]"*, thereby disallowing non-persistent copies that are overwritten on a periodic basis, resulting in a much shorter retention period than the original.

2.5.2 Compliance Assessment

Cohasset upholds that the functionality of Amazon S3 meets both paragraphs (A) and (B) of this SEC requirement by retaining a persistent duplicate copy of the records or alternate source to reestablish the records, when (a) properly configured with Cross-Region Replication (CRR) as described in Section 2.5.3 and (b) the considerations described in Section 2.5.4 are satisfied.

2.5.3 Amazon S3 Capabilities

The two options for meeting the record redundancy requirement are described in the following subsections.

2.5.3.1 Redundant Set of Records

- Optionally, the regulated entity may configure Buckets with Cross-Region Replication (CRR) to enable automatic, asynchronous copying of objects, and associated metadata, to Buckets in different AWS Regions.

[13] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66421.

[14] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66421.

The CRR configuration may apply to an entire Bucket or to select criteria, e.g., Object Key Name prefix or Amazon S3 tags may define specific objects to be replicated from the source to the target Bucket.

- When utilizing CRR to meet this requirement to maintain a duplicate of the objects: (a) both the source and the target Buckets must be configured for compliance with the SEC Rules and (b) the retention controls (*Object Lock* mode, *Retain Until Date* and *Legal Hold* status) applied to objects stored in the source Bucket must comply with the SEC Rules. See Section 2.2, *Non-Rewriteable, Non-Erasable Record Format*, for additional information.
- Objects that meet the CRR criteria replicate from the source Bucket to the target Bucket, together with retention controls (*Object Lock* mode, *Retain Until Date* and *Legal Hold* status) and other metadata.
  - Objects *added* to the source Bucket after CRR is configured are automatically replicated, if the object meets the CRR criteria.
- When the retention controls of replicated objects are updated in the source Bucket (e.g., a *Retain Until Date* is extended or a *Legal Hold* status is changed), the updated metadata is automatically synchronized to the object in the target Bucket. (See Section 2.2.3.3, *Record Definition and Retention Controls*, for a description of allowed changes to retention controls for objects with an *Object Lock* mode set to *Compliance* or *Governance*.)
  - Note: Retention settings updated on the target Bucket do not synchronize to the source Bucket. Accordingly, to assure the same settings in both Buckets, Cohasset recommends all retention control changes be made to objects in the source Bucket, for automatic synchronization to the target Bucket.
- When replication fails, the configuration that caused the failure must be corrected. Thereafter, to replicate the object, either:
  - Create a new version of the object, which will then replicate. Note: Each version is stored with a system-defined, immutable creation/storage timestamp.
  - Contact AWS Support to clear the replication status on the specific object that failed to replicate.

2.5.3.2 Other Redundancy Capabilities

- As a standard service, Amazon S3 redundantly stores objects on multiple devices across multiple facilities in an AWS region. When an object is uploaded to Amazon S3, data is synchronously stored across multiple facilities before a *success* response is returned.
  - Standard Amazon S3 storage is backed by the Amazon S3 Service Level Agreement and is designed to (a) sustain the concurrent loss of data in two facilities and (b) provide 99.999999999% (11-nines) durability and 99.99% availability of objects over a given year.
  - Over the lifespan of the object, Amazon S3 automatically regenerates an accurate replica of the object and associated metadata in the event the original is lost or damaged.

2.5.4 Additional Considerations

In addition, for this requirement, the regulated entity is responsible for: (a) maintaining its account in good standing and (b) maintaining the technology, storage capacity, encryption keys, and other information and services needed to use Amazon S3 and permit access to the redundant records.

Further, if CRR will be used for compliance with this requirement of the Rule to maintain a duplicate of the objects, the regulated entity is responsible for: (a) properly configuring CRR services, (b) correcting any errors resulting from CRR replication configurations, and (c) validating that the retention controls applied to objects in both the source and target Buckets are appropriate. Cohasset recommends: (a) configuring the source and target Buckets with the same retention controls and (b) making all changes to retention controls only in the source Bucket.

2.6 Audit System

2.6.1 Compliance Requirement

For electronic recordkeeping systems that comply with the non-rewriteable, non-erasable format requirement, as stipulated in Section 2.2, *Non-Rewriteable, Non-Erasable Record Format*, the Rules require the regulated entity to maintain an audit system for accountability (e.g., when and what action was taken) for both (a) inputting each record and (b) tracking changes made to every original and duplicate record. Additionally, the regulated entity must ensure the audit system results are available for examination for the required retention time period stipulated for the record.

SEC 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii):

For a [regulated entity] operating pursuant to paragraph [(f)(2)(i)(B) or (e)(2)(i)(B)] of this section, the [regulated entity] must have in place an audit system providing for accountability regarding inputting of records required to be maintained and preserved pursuant to [§ 240.17a-3 or § 240.18a-5] and this section to the electronic recordkeeping system and inputting of any changes made to every original and duplicate record maintained and preserved thereby.

(A) At all times, a [regulated entity] must be able to have the results of such audit system available for examination by the staffs of the Commission [and other pertinent regulators].

(B) The audit results must be preserved for the time required for the audited records

The audit results may be retained in any combination of audit systems utilized by the regulated entity.

2.6.2 Compliance Assessment

Cohasset asserts that Amazon S3, in conjunction with the AWS CloudTrail service, when enabled, supports the regulated entity's efforts to meet this SEC requirement for an audit system.

2.6.3 Amazon S3 Capabilities

The regulated entity is responsible for an audit system, and compliance is supported by Amazon S3.

- For each record stored, Amazon S3 retains the following audit information.
  - A unique **Object Key Name** which is comprised of the Bucket name, prefix and object name. Note: the Bucket name must be globally unique across Amazon S3, and the object name must be unique within the Bucket.
  - A **version identifier**, which is automatically incremented with each new version of the object.
  - The **creation/storage timestamp**.

  This metadata is *immutably* stored for the lifespan of the record and is produced together with the record.

- The record is immutable, meaning modifications are disallowed; therefore, tracking of the inputting of changes made is not relevant to Amazon S3. Note: When the record is protected with less-restrictive *Governance* mode retention controls, the retention controls may be circumvented by administrators with *BypassGovernanceRetention* permission, thus allowing for the premature deletion of the record.
- Amazon also provides AWS CloudTrail which is a highly configurable service that monitors and records API calls and user activity within an AWS account.
  - By default, management events within a given AWS Region are captured and immutably retained in an S3 Bucket for 90 days. Types of events captured include AWS IAM security configurations, creating Buckets, deleting Buckets, creating Bucket lifecycle policies, enabling *Object Lock* on a Bucket, applying Bucket policies, and administrative actions taken using the *BypassGovernanceMode* permission.
    - Management event history is viewable with limited search and filter options via the CloudTrail console or via API and CLI commands.
  - The regulated entity may opt-in to additional CloudTrail features to capture data events (i.e., object-level operations), including the initial recording of an object, applying a *Retain Until Date*, extending retention, applying a legal hold, and deleting an object.
    - Data events may be queried via API or CLI commands, however, they are not viewable via the CloudTrail console.
- To retain CloudTrail data for longer than the default 90 days, Amazon offers the following options:
  - *CloudTrail Lake event data stores* (i.e., managed data lakes, optimized for fast retrieval and analysis) can be configured to retain both management and data events, in addition to other types of data logs, from the current AWS Region or from all AWS Regions within an AWS account. Events stored in the data store may be retained for up to ten years, during which time the data is available for advanced queries. Query results can be saved to an S3 Bucket or downloaded to a CSV file for export to an external security information event management (SIEM) tool.
  - *CloudTrail "trails"* may be configured to capture management and data events and deliver them directly (a) to an S3 Bucket, where they may be viewed and/or downloaded or (b) to an external SIEM tool. Trails may be configured for a single AWS Region, multiple AWS Regions, or for an entire AWS Organization.

2.6.4 Additional Considerations

The regulated entity is responsible for maintaining an audit system for inputting records and changes made to the records. In addition to relying on the immutable metadata, the regulated entity may utilize the AWS CloudTrail service. When relying on the AWS CloudTrail service, Cohasset recommends using either (a) the CloudTrail Lake event data store service which provides long-term, immutable retention of event data or (b) the CloudTrail trails service which allows for the export of audit events to a secure S3 Bucket or an external SIEM tool.

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

This section contains a summary assessment of the functionality of Amazon S3, as described in Section 1.3, *Amazon S3 Overview and Assessment Scope*, in comparison to CFTC electronic regulatory record requirements. Specifically, this section associates the features described in Section 2, *Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e),* with the principles-based requirements of CFTC Rule 1.31(c)-(d).

Cohasset's assessment, enumerated in Section 2, pertains to the electronic recordkeeping system requirements of SEC Rules 17a-4(f)(2) and 18a-6(e)(2) and the associated SEC interpretations, as well as the audit system requirement of SEC Rules 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii).

In the October 12, 2022 adopting release, the SEC recognizes the CFTC principles-based requirements and asserts a shared objective of ensuring the authenticity and reliability of regulatory records. Moreover, the SEC contends that its two compliance alternatives, i.e., (1) record and audit-trail and (2) non-rewriteable, non-erasable record format, a.k.a. WORM, are more likely to achieve this objective because each alternative requires the specific and testable outcome of accessing and producing modified or deleted records, in their original form, for the required retention period.

> *The proposed amendments to Rules 17a-4 and 18a-6 and the [CFTC] principles-based approach recommended by the commenters share an objective: ensuring the authenticity and reliability of regulatory records. However, the audit-trail requirement is more likely to achieve this objective because, like the existing WORM requirement, it sets forth a specific and testable outcome that the electronic recordkeeping system must achieve: the ability to access and produce modified or deleted records in their original form.*[15] [emphasis added]

In Section 2 of this report, Cohasset assesses Amazon S3 with the *Object Lock* feature applied in (1) *Compliance* mode, a highly-restrictive option that provides both overwrite protection and strict retention controls, and (2) *Governance* mode, a less-restrictive option, which provides overwrite protection but requires administrative procedures and monitoring to ensure compliant retention, since privileged administrators are allowed to shorten or remove retention controls. (See Section 2.2, *Non-Rewriteable, Non-Erasable Record Format*, for information on the two *Object Lock* modes.)

In the following table, Cohasset correlates specific *principles-based* CFTC requirements for electronic records with the assessed functionality of Amazon S3.

[15] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.

CFTC 1.31(c)-(d) Regulation [emphasis added]	**Compliance Assessment Relative to CFTC 1.31(c)-(d)**
(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 the CFTC requirements in (c)(1) and (c)(2)(i), for records[16] with time-based retention periods, are met by the functionality of Amazon S3, with the *Object Lock* feature. The functionality that supports retention, authenticity and reliability of electronic records is described in the following sections of this report: ● Section 2.2, *Non-Rewriteable, Non-Erasable Record Format* ● Section 2.3, *Record Storage Verification* ● Section 2.4, *Capacity to Download and Transfer Records and Location Information* ● Section 2.6, *Audit System* Additionally, for *records stored electronically*, the CFTC definition of *regulatory records* in 17 CFR § 1.31(a) includes information to access, search and display records, as well as data on records creation, formatting and modification: *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] Amazon S3 retains immutable metadata (e.g., Object Key Name, version identifier and creation/storage timestamp) as an integral component of the records, and, therefore, these attributes are subject to the same retention controls as the associated record. These immutable attributes support both (a) records access, search and display and (b) audit system and accountability for inputting the records. Additionally, mutable metadata stored for records include retention controls (e.g., *Retain Until Date*) and legal hold attributes. The most recent values of mutable metadata are retained for the same time period as the associated records. Further, Amazon S3 in conjunction with the CloudTrail service, tracks management and data audit events and provides storage options for retaining this additional audit system information for the same time period as the record. For additional information, see Section 2.6, *Audit System*.
(ii) Systems that ensure the records entity is able to produce electronic regulatory records 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 Amazon S3 capabilities described in Section 2.5, *Record Redundancy*, including methods for a persistent duplicate copy as well as an alternate source to reestablish the records and associated system metadata, 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*.

[16] The regulated entity is responsible for retaining and managing any additional required information, such as information to augment search and data on how and when the records were created, formatted, or modified, in a compliant manner.

CFTC 1.31(c)-(d) Regulation [emphasis added]	**Compliance Assessment Relative to CFTC 1.31(c)-(d)**
(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).
(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 Amazon S3 has features that support the regulated entity's efforts to comply with requests for inspection and production of records, as described in. ● Section 2.2, *Non-Rewriteable, Non-Erasable Record Format* ● Section 2.4, *Capacity to Download and Transfer Records and Location Information* ● Section 2.6, *Audit System*

4 • Conclusions

Cohasset assessed the functionality of Amazon S3[17] in comparison to the electronic recordkeeping system requirements set forth in SEC Rules 17a-4(f)(2) and 18a-6(e)(2) and described audit system features that support the regulated entity as it meets the requirements of SEC Rules 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii).

Cohasset determined that Amazon S3, when properly configured, has the following functionality, which meets the regulatory requirements:

- Maintains records and certain associated metadata in a non-erasable and non-rewriteable format for time-based retention periods, when a *Retain Until Date* is applied and the *Object Lock* mode is set to either *Compliance* or *Governance* mode.
- Allows a *Legal Hold* status to be applied to objects subject to preservation requirements, which retains (preserves) the object as immutable and prohibits deletion or overwrites until the *Legal Hold* status is disabled.
- Prohibits deletion of a record and its immutable metadata until the applied *Retain Until Date* has expired.
- Encrypts objects at rest (data stored in Amazon S3 data centers) by default and supports encryption of data in-transit (data traveling to and from Amazon S3) using SSL (Secure Sockets Layer) or by client-side encryption.
- Verifies the accuracy and quality of the recording process automatically utilizing (a) advanced storage recording technology and (b) a checksum that must be received from the source system, if retention controls are applied to the object during the recording process. The checksum is stored as metadata and utilized for post-recording verification.
- Allows authorized users to access the records and metadata with Amazon S3 API, CLI or Management Console for local reproduction or transfer to a format and medium acceptable under the Rule.
- Regenerates an accurate replica of records and metadata from redundant objects, should data be lost or damaged. Offers optional Cross-Regional Replication to automatically, asynchronously copy records, and associated metadata, to Buckets in different AWS Regions.

Accordingly, Cohasset concludes that Amazon S3, when properly configured and the additional considerations are satisfied, meets the electronic recordkeeping system requirements of SEC Rules 17a-4(f)(2) and 18a-6(e)(2) and FINRA Rule 4511(c), as well as supports the regulated entity in its compliance with the audit system requirements in SEC Rules 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii). In addition, the assessed capabilities meet the principles-based electronic records requirements of CFTC Rule 1.31(c)-(d).

[17] See Section 1.3, *Amazon S3 Overview and Assessment Scope*, for an overview of the solution and the scope of deployments included in the assessment.

Appendix A • Overview of Relevant Electronic Records 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 electronic records retained on compliant electronic recordkeeping systems.

A.1 Overview of SEC Rules 17a-4(f) and 18a-6(e) *Electronic Recordkeeping System* Requirements

In 17 CFR §§ 240.17a-3 and 240.17a-4 for securities broker-dealer industry and 17 CFR §§ 240.18a-5 and 240.18a-6 for nonbank SBS entities, the SEC stipulates recordkeeping requirements, including retention periods.

Effective January 3, 2023, the U.S. Securities and Exchange Commission (SEC) promulgated amendments[18] to 17 CFR § 240.17a-4 (Rule 17a-4) and 17 CFR § 240.18a-6 (Rule 18a-6), which define more technology-neutral requirements for electronic recordkeeping systems.

> *The objective is to prescribe rules that remain workable as record maintenance and preservation technologies evolve over time but also to set forth requirements designed to ensure that broker-dealers and SBS Entities maintain and preserve records in a manner that promotes their integrity, authenticity, and accessibility.*[19] [emphasis added]

These 2022 amendments (a) provide a record and complete time-stamped audit-trail alternative and (b) allow regulated entities to continue using the electronic recordkeeping systems they currently employ to meet the non-rewriteable, non-erasable (i.e., WORM or write-once, read-many) requirement.

> *Under the final amendments, broker-dealers and nonbank SBS Entities have the flexibility to preserve all of their electronic Broker-Dealer Regulatory Records or SBS Entity Regulatory Records either by: (1) using an electronic recordkeeping system that meets either the audit-trail requirement or the WORM requirement; or (2) preserving some electronic records using an electronic recordkeeping system that meets the audit-trail requirement and preserving other electronic records using an electronic recordkeeping system that meets the WORM requirement.*[20] [emphasis added]

The following sections separately address (a) the record and audit-trail and (b) the non-rewriteable, non-erasable record format alternatives for compliant electronic recordkeeping systems.

A.1.1 Record and Audit-Trail Alternative

The objective of this requirement is to allow regulated entities to keep required records and complete time-stamped record audit-trails in business-purpose recordkeeping systems.

[18] The compliance dates are May 3, 2023, for 17 CFR § 240.17a-4, and November 3, 2023, for 17 CFR § 240.18a-6.

[19] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66428.

[20] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66419.

> *[T]o preserve Broker-Dealer Regulatory Records and SBS Regulatory Records, respectively, on the same electronic recordkeeping system they use for business purposes, but also to require that the system have the capacity to recreate an original record if it is modified or deleted. This requirement was designed to provide the same level of protection as the WORM requirement, which prevents records from being altered, over-written, or erased.*[21] [emphasis added]

The complete time-stamped audit-trail must both (a) establish appropriate systems and controls that ensure the authenticity and reliability of required records and (b) achieve the testable outcome of accessing and reproducing the original record, if modified or deleted during the required retention period, without prescribing how the system meets this requirement.

> *[L]ike the existing WORM requirement, [the audit-trail requirement] sets forth a specific and testable outcome that the electronic recordkeeping system must achieve: the ability to access and produce modified or deleted records in their original form.*[22] [emphasis added]

Further, the audit-trail applies only to required records: *"the audit-trail requirement applies to the final records required pursuant to the rules, rather than to drafts or iterations of records that would not otherwise be required to be maintained and preserved under Rules 17a-3 and 17a-4 or Rules 18a-5 and 18a-6."*[23] [emphasis added]

A.1.2 Non-Rewriteable, Non-Erasable Record Format Alternative

With regard to the option of retaining records in a non-rewriteable, non-erasable format, the adopting release clarifies that the previously released interpretations to both SEC Rules 17a-4(f) and 18a-6(e) still apply.

> *The Commission confirms that a broker-dealer or nonbank SBS Entity can rely on the 2003 and 2019 interpretations with respect to meeting the WORM requirement of Rule 17a-4(f) or 18a- 6(e), as amended.*
> *****
> *In 2001, the Commission issued guidance that Rule 17a-4(f) was consistent with the ESIGN Act. The final amendments to Rule 17a-4(f) do not alter the rule in a way that would change this guidance. Moreover, because Rule 18a-6(e) is closely modelled on Rule 17a-4(f), it also is consistent with the ESIGN Act****[24] [emphasis added]

In addition to the Rules, the following interpretations are extant and apply to both SEC Rules 17a-4(f) and 18a-6(e).

- *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), Exchange Act Release No. 44238 (May 1, 2001), 66 FR 22916 (May 7, 2001)* (2001 Interpretative Release).
- *Electronic Storage of Broker-Dealer Records, Exchange Act Release No. 47806 (May 7, 2003), 68 FR 25281, (May 12, 2003)* (2003 Interpretative Release).
- *Recordkeeping and Reporting Requirements for Security-Based Swap Dealers, Major Security Based Swap Participants, and Broker-Dealers, Exchange Act Release No. 87005 (Sept. 19, 2019), 84 FR 68568 (Dec. 16, 2019)* (2019 SBSD/MSBSP Recordkeeping Adopting Release).

---

21 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.
22 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.
23 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66418.
24 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66419.

The 2003 Interpretive Release allows rewriteable and erasable media to meet the non-rewriteable, non-erasable requirement, if the system delivers the prescribed functionality, using appropriate integrated control codes.

> *A broker-dealer would not violate the requirement in paragraph* [(f)(2)(i)(B) (refreshed citation number)] *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.*[25] [emphasis added]

Further, the 2019 interpretation clarifies that solutions using only software control codes also meet the requirements of the Rules:

> *The Commission is clarifying that a software solution that prevents the overwriting, erasing, or otherwise altering of a record during its required retention period would meet the requirements of the rule.*[26] [emphasis added]

The term *integrated* means that the method used to achieve non-rewriteable, non-erasable preservation must be an integral part of the system. The term *control codes* indicates the acceptability of using attribute codes (metadata), which are integral to the software controls or the hardware controls, or both, which protect the preserved record from overwriting, modification or erasure.

The 2003 Interpretive Release is explicit that merely mitigating (rather than preventing) the risk of overwrite or erasure, such as relying solely on passwords or other extrinsic security controls, will not satisfy the requirements.

Further, the 2003 Interpretive Release requires the capability to retain a record beyond the SEC-established retention period, when required by a subpoena, legal hold or similar circumstances.

> *[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.*[27] [emphasis added]

See Section 2, *Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e),* for each SEC electronic recordkeeping system requirement and a description of the functionality of Amazon S3 related to each requirement.

A.2 Overview of FINRA Rule 4511(c) *Electronic Recordkeeping System* Requirements

Financial Industry Regulatory Authority (FINRA) Rules regulate member brokerage firms and exchange markets. Additionally, FINRA adopted amendments clarifying the application of FINRA Rules to security-based swaps (SBS).[28]

FINRA Rule 4511(c) explicitly defers to the requirements of SEC Rule 17a-4, for 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.*

---

25 2003 Interpretative Release, 68 FR 25282.

26 Recordkeeping and Reporting Requirements for Security-Based Swap Dealers, Major Security- Based Swap Participants, and Broker-Dealers, Exchange Act Release No. 87005 (Sept. 19, 2019), 84 FR 68568 (Dec. 16, 2019) (2019 SBSD/MSBSP Recordkeeping Adopting Release).

27 2003 Interpretative Release, 68 FR 25283.

28 FINRA, Regulatory Notice 22-03 (January 20, 2022), FINRA Adopts Amendments to Clarify the Application of FINRA Rules to Security-Based Swaps.

A.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 modernize and make technology-neutral the form and manner in which to keep regulatory records. This resulted in less-prescriptive, principles-based requirements.

> *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.*[29] [emphasis added]

The following definitions in 17 CFR § 1.31(a) confirm that recordkeeping obligations apply to all *records entities* and 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.

> *Definitions. For purposes of this section:*
>
> *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]

The retention time periods for required records includes both time-based and event-based retention periods. Specifically, 17 CFR § 1.31(b) 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.*
>
> *(4) A records entity shall keep regulatory records exclusively created and maintained on paper readily accessible for no less than two years. A records entity shall keep electronic regulatory records readily accessible for the duration of the required record keeping period.* [emphasis added]

For a list of the CFTC principles-based requirements and a summary assessment of Amazon S3 in relation to each requirement, see Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*.

[29] Recordkeeping, 82 FR 24482 (May 30, 2017) (2017 CFTC Adopting Release).

Appendix B • Cloud Provider Undertaking

B.1 Compliance Requirement

Separate from the electronic recordkeeping system requirements described in Section 2, *Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e),* the SEC requires submission of an undertaking when records are stored on systems owned or operated by a party other than the regulated entity.

The purpose of the undertaking is to ensure the records are accessible and can be examined by the regulator.

SEC Rules 17a-4(i)(1)(ii) and 18a-6(f)(1)(ii) explain an 'Alternative Undertaking,' which applies to cloud service providers if the regulated entity has 'independent access' to records, which allows it to (a) regularly access the records without relying on the cloud service provider to take an intervening step to make the records available, (b) allow regulators to examine the records, during business hours, and (c) promptly furnish the regulator with true, correct, complete and current hard copy of the records.

This undertaking requires the cloud service provider (a) facilitate the process, (b) not block access, and (c) not impede or prevent the regulated entity or the regulator itself from accessing, downloading, or transferring the records for examination.

> *These undertakings are designed to address the fact that, while the broker-dealer or SBS Entity has independent access to the records, the third party owns and/or operates the servers or other storage devices on which the records are stored. Therefore, the third party can block records access. In the Alternative Undertaking, the third party will need to agree not to take such an action. Further, the third party will need to agree to facilitate within its ability records access. This does not mean that the third party must produce a hard copy of the records or take the other actions that are agreed to in the Traditional Undertaking. Rather, it means that the third party undertakes to provide to the Commission*

SEC 17a-4(i)(1)(ii) and 18a-6(f)(1)(ii):

(A) If the records required to be maintained and preserved pursuant to the provisions of [§ 240.17a-3 or § 240.18a-5] and this section are maintained and preserved by means of an electronic recordkeeping system as defined in paragraph [(f) or (e)] of this section utilizing servers or other storage devices that are owned or operated by an outside entity (including an affiliate) and the [regulated entity] has independent access to the records as defined in paragraph [(i)(1)(ii)(B) or (f)(1)(ii)(B)] of this section, the outside entity may file with the Commission the following undertaking signed by a duly authorized person in lieu of the undertaking required under paragraph [(i)(1)(i) or (f)(1)(i)] of this section:

> The undersigned hereby acknowledges that the records of [regulated entity] are the property of [regulated entity] and [regulated entity] has represented: one, that it is subject to rules of the Securities and Exchange Commission governing the maintenance and preservation of certain records, two, that it has independent access to the records maintained by [name of outside entity], and, three, that it consents to [name of outside entity or third party] fulfilling the obligations set forth in this undertaking. The undersigned undertakes that [name of outside entity or third party] will facilitate within its ability, and not impede or prevent, the examination, access, download, or transfer of the records by a representative or designee of the Securities and Exchange Commission as permitted under the law. *****

(B) A [regulated entity] utilizing servers or other storage devices that are owned or operated by an [outside entity or third party] has independent access to records with respect to such [outside entity or third party] if it can regularly access the records without the need of any intervention of the [outside entity or third party] and through such access:

(1) Permit examination of the records at any time or from time to time during business hours by representatives or designees of the Commission; and

(2) Promptly furnish to the Commission or its designee a true, correct, complete and current hard copy of any or all or any part of such records [emphasis added]

representative or designee or SIPA trustee the same type of technical support with respect to records access that it would provide to the broker-dealer or SBS Entity in the normal course.[30] [emphasis added]

B.2 Amazon Undertaking Process

The regulated entity and Amazon collaborate to reach agreement on the scope, terms and conditions of the undertaking.

- The undertaking requires actions be taken by both parties:
  1. The regulated entity affirms, in writing, it:
     - Is subject to SEC Rules 17a-3, 17a-4, 18a-5 or 18a-6 governing the maintenance and preservation of certain records,
     - Has independent access to the records maintained on Amazon S3, and
     - Consents to Amazon fulfilling the obligations set forth in this undertaking.
  2. Amazon:
     - Acknowledges that the records are the property of the regulated entity,
     - For the duration of the undertaking, agrees to facilitate within its ability, and not impede or prevent, the examination, access, download, or transfer of the records by a regulatory or trustee, as permitted under the law, and
     - Prepares the undertaking, utilizing the explicit language in the Rule, then submits, via email, the undertaking to the SEC.
- Important Note: While Amazon provides this undertaking to the SEC on behalf of the regulated entity, the regulated entity is not relieved from its responsibility to prepare and maintain required records.

B.3 Additional Considerations

The regulated entity is responsible for (a) initiating the undertaking, (b) reaching agreement with Amazon on the scope, terms, and conditions of the undertaking, (c) maintaining its account in good standing, (d) implementing and configuring the cloud services to ensure its records are maintained and preserved as required by applicable laws and regulations, (e) maintaining technology, encryption keys and privileges to access Amazon S3, and (f) assuring that the regulator has (when needed) access privileges, encryption keys, and other information and services to permit records to be accessed, downloaded, and transferred.

[30] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66429.

About Cohasset Associates, Inc.

Cohasset Associates, Inc. (www.cohasset.com) is a professional consulting firm, specializing in records management and information governance. Drawing on more than fifty 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, designing and supporting implementations that promote interdisciplinary information governance, achieve business objectives, optimize information value, improve compliance, and mitigate information-related risk.

Cohasset is 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.

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

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 supports the implementation of information lifecycle practices that mitigate the cost and risk associated with over-retention*
- *Defines strategy and design for information governance in collaboration tools, such as M365*
- *Defines technical and functional requirements and assists with the deployment of enterprise content management and collaboration tools*

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.