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 requiring fixed (time-based) or variable (event-based) retention 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).

This report assesses both **fixed** and **variable** Object Lock retention features. It is Cohasset's opinion that Amazon S3, when properly configured and used with the Object Lock features and other compliance capabilities, 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.

September 2026

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

+1.312.527.1550 | Visit Cohasset website

Table of Contents

Abstract **1**

Table of Contents **2**

1 • Introduction **3**

1.1 Overview of the Regulatory Requirements 3

1.2 Purpose and Approach 4

1.3 Amazon S3 Overview and Assessment Scope 5

2 • Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e) **7**

2.1 Record and Audit Trail 7

2.2 Non-Rewriteable, Non-Erasable Record Format 8

2.3 Record Storage Verification 25

2.4 Capacity to Download and Transfer Records and Location Information 26

2.5 Record Redundancy 28

2.6 Audit System 30

3 • Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d) **33**

4 • Conclusions **36**

Appendix A • Guidance for Applying Object Lock Controls **37**

A.1 Guidance for Fixed Retention Controls 37

A.2 Guidance for Variable Retention Controls 43

A.3 Condition Keys for Bucket and IAM Policies 55

Appendix B • Overview of Relevant Electronic Records Requirements **57**

B.1 Overview of SEC Rules 17a-4(f) and 18a-6(e) *Electronic Recordkeeping System* Requirements 57

B.2 Overview of FINRA Rule 4511(c) *Electronic Recordkeeping System* Requirements 59

B.3 Overview of CFTC Rule 1.31(c)-(d) *Electronic Regulatory Records* Requirements 60

Appendix C • Cloud Provider Undertaking **61**

C.1 Compliance Requirement 61

C.2 Amazon Undertaking Process 62

C.3 Additional Considerations 62

About Cohasset Associates, Inc. **63**

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-4 (SEC Rule 17a-4) for the securities broker-dealer industry and 17 CFR § 240.18a-6 (SEC Rule 18a-6) for nonbank SBS entities,[1] the U.S. Securities Exchange Commission (SEC) stipulates recordkeeping requirements, including retention periods.

In 2022, the SEC adopted amendments to SEC Rules 17a-4 and 18a-6, establishing technology-neutral 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 B.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

In 17 CFR § 1.31 (CFTC Rule 1.31), the U.S. Commodity Futures Trading Commission (CFTC) stipulates recordkeeping requirements, including retention periods.

In 2017, the CFTC adopted amendments to CFTC Rule 1.31, establishing principles-based, technology-neutral requirements for electronic regulatory records.

> *The Commodity Futures Trading Commission (the "Commission") is amending the recordkeeping obligations set forth in Commission regulations *** The amendments modernize and make technology neutral the form and manner in which regulatory records must be kept **** [4] [emphasis added]

For additional information, refer to Section 3, *Summary Assessment of* Compliance *with CFTC Rule 1.31(c)-(d)*, and Appendix B.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

[4] Commodity Futures Trading Commission, Amendments to Recordkeeping Requirements, 82 FR 24479 (May 30, 2017). (2017 CFTC Recordkeeping Requirements Adopting Release).

documentation, (c) product demonstrations, including system setup and configuration, (d) 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[5] 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 fixed[6] or variable[7] retention period and legal holds.

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

- An AWS Organization has one AWS **Management Account** that is used to centrally manage all Member Accounts and apply organization-wide policies and governance controls.
- **Organizational Units** are logical containers used to hierarchically group Member Accounts.
- A **Member Account** is an AWS account that is assigned to one Organizational Unit at a time. Specific resources, identity and access management and configurations are assigned to the Member Account, which is subject to governance controls and policies inherited from the Organizational Unit and Management Account where it resides. A Member Account may have Amazon S3 with multiple S3 buckets as one of its services.

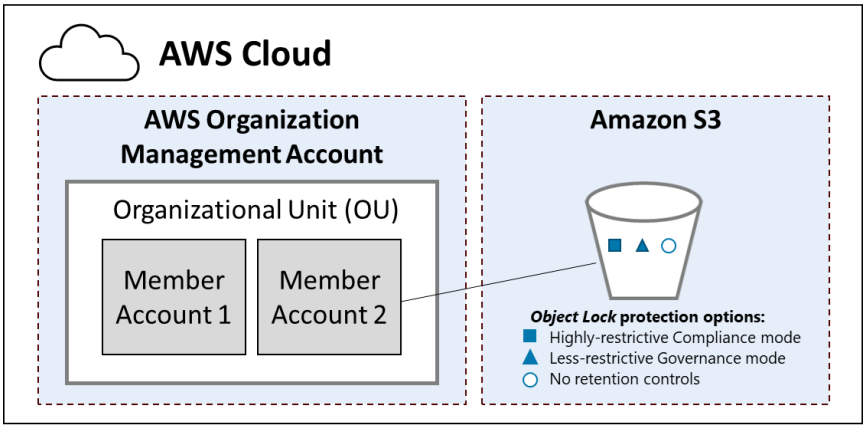


Figure 1: Amazon S3 Storage Hierarchy

5 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.

6 Fixed (i.e., time based) retention periods require records to be retained until a specific date in the future (i.e., for a fixed contiguous period of time from the creation or storage timestamp).

7 Variable (i.e., event based) retention periods require records to be retained indefinitely until a specified business event occurs i(e.g., a contract expires or an employee terminates), after which the record is retained for a fixed retention period.

Amazon S3 is an object storage service. **Buckets** are cloud storage resources that serve as logical containers for storing individual versions of objects (i.e., records). For buckets intended to retain records in a non-erasable and non-rewriteable format for fixed and/or variable retention periods in compliance with SEC Rules, 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 reduce or remove retention controls and prematurely delete required records.

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).
  - AWS cloud environments that are provided and operated by companies other than Amazon Web Service., e.g., AWS services in mainland China.
  - 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 set forth 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 allow regulated entities to use business-purpose electronic recordkeeping systems to achieve the required outcome without specifying a particular technology.

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 explains 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.*[8] [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.*[9] [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 electronic 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 electronic recordkeeping 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.

8 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.

9 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66418.

> *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 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.*[10] [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.*[11] [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 fixed[12] and variable[13] retention periods and legal holds, when (a) properly configured, as described in Section 2.2.3 and (b) the additional 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.

---

10 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66419.

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

12 Fixed (i.e., time based) retention periods require records to be retained until a specific date in the future, (i.e., for a fixed contiguous period of time from the creation or storage timestamp).

13 Variable (i.e., event based) retention periods require records to be retained indefinitely until a specified business event occurs (e.g., a contract expires or an employee terminates), after which the record is retained for a fixed retention period.

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.
- Amazon S3 provides two Object Lock features for the immutable preservation of records, when stored in buckets with the Amazon S3 Object Lock feature enabled (On):

    1. **Object Lock Retention**: To meet the requirements of SEC Rules 17a-4(f) and 18a-6(e), the appropriate type of Object Lock retention controls must be stored as metadata for each object version that is a required record.

        - **Fixed retention** requires storing version metadata for (a) **Object Lock Mode**, in either highly restrictive Compliance mode or less restrictive Governance mode and (b) a **Retain Until Date** that is in the future. The Retain Until Date may be system calculated or transmitted with the version.
        - **Variable retention** requires storing version metadata for (a) **Object Lock Mode**, in either highly restrictive Compliance mode or less restrictive Governance mode, (b) **Event Hold** set to On to activate variable retention, (c) **Event Hold Duration**, specified in days or years, and (d) a **Retain Until Date** that is in the future. The Retain Until Date may be system calculated or transmitted with the version.

    2. **Object Lock Legal Hold**: Optionally, a **Legal Hold** may be set (On) on any object version to suspend eligibility for deletion until the Legal Hold is cleared (Off).

- The following table summarizes the Object Lock controls, when applied in either Compliance or Governance mode. See the subsections following this *Overview*, for information on configuring the Object Lock 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 (i.e., version) and its immutable metadata cannot be modified for its lifespan. • The versioning feature, which is required when using Object Lock, ensures that stored versions are not modified or overwritten; instead, a new version is created, with separate Object Lock retention and Legal Hold values. • Renaming buckets, objects, and version identifiers is prohibited.	
Restricting changes to applied retention controls	• For versions in Compliance mode, authorized users and Lifecycle policies are prohibited from changing a version's retention controls to be less restrictive. Accordingly, Compliance mode ensures that Object Lock retention controls are not circumvented by any user or process. • See Section 2.2.3.3, *Record Definition and Object Lock Controls.*	• For versions in Governance mode, users without the *BypassGovernanceRetention* permission are subject to the same controls as described for Compliance mode. • However, users with *BypassGovernanceRetention* permissions may: ○ Reduce the Retain Until Date. ○ Remove the Object Lock Governance mode and the retention controls, entirely. ○ Change Object Lock Mode from Governance to Compliance and update the Retain Until Date. Accordingly, procedural controls and monitoring are required to scrutinize privileged administrator actions taken to change or remove Object Lock retention controls.

	Object Lock, in highly restrictive Compliance mode	Object Lock, in less restrictive Governance mode
Applying and removing legal holds	• A Legal Hold may be set (On) which prevents deletion of that version until the Legal Hold is cleared (Off). • See Section 2.2.3.4, *Legal Holds (Temporary Holds).*	
Restricting deletion of records and buckets	• A specific record (i.e., version) can be deleted when its: ○ Retain Until Date has expired, and ○ Event Hold is cleared (Off) or not set, and ○ Legal Hold is cleared (Off) or not set. • 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.*	• For versions in Governance mode, Lifecycle policies and users without the *BypassGovernanceRetention* permission are subject to the same controls as described for Compliance mode. • Users with the *BypassGovernanceRetention* permission may delete an unexpired object version, if the version's Legal Hold status is Off or not set. Accordingly, procedural controls and monitoring are required to scrutinize privileged administrator actions to prematurely delete records.

► The features and protections listed above apply across all Amazon S3 storage classes, including the S3 Glacier storage classes[14] (archival storage). Therefore, Lifecycle policies may be used to tier protected objects in Amazon S3 storage classes.

2.2.3.2 Amazon S3 Immutability and Retention Configurations

► The following table describes S3 bucket, policies for S3 buckets and Identity and Access Management (IAM), and Lifecycle configurations related to the S3 Object Lock feature. See Section 2.2.3.3, *Record Definition and Object Lock 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	• By default, Amazon S3 general purpose bucket names must be unique across all AWS accounts and all AWS Regions within an AWS partition. Additionally, Amazon S3 supports account regional namespaces, in which bucket names must be unique within the account regional namespace rather than the shared global namespace.
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 the Object Lock **feature** and versioning are enabled, versioning cannot be suspended or disabled. ○ New object versions are created with write operations such as (a) write a new version, (b) update user-defined metadata (i.e., name-value pairs) and (c) copy an object. ▪ Additionally, a new version must be stored to create, update or delete a version's annotations, if the version is protected with Object Lock retention controls in either Compliance or Governance modes. Users with *BypassGovernanceRetention* permission cannot override the restrictions on annotation operations. ○ New object versions are not created when changing Object Lock retention or Legal Hold values for an object version. Additionally, changes 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 values. When controls are set without specifying a version, the controls apply to the current (top) version.

[14] 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.

<table>
<tr><th></th><th>Bucket, IAM Policy and Lifecycle Policy Configurations related to S3 Object Lock</th></tr>
<tr><td>Bucket default retention configurations</td><td>

Bucket defaults may be configured to automatically apply retention controls to each version being stored, unless Object Lock retention and/or Legal Hold values are explicitly transmitted with the version. Important Note: Legal Holds are an Object Lock control; therefore, if an object version is transmitted with only a Legal Hold status of On or Off, bucket retention defaults are not applied.
The following sub-tables describe the recommended default configurations for applying fixed and variable retention in compliance with SEC Rules.

<table>
<tr><th>Fixed retention (Configure bucket defaults for Object Lock Mode and Retention Period)</th></tr>
<tr><td>

Configure the following bucket defaults for buckets that will store records requiring a fixed retention period (e.g., 6 Years).

Configure Default Object Lock Mode to either Compliance (highly restrictive) or Governance (less restrictive).
Configure the Default Retention Period to a value between 1 day and 100 years, that satisfies retention requirements and any applicable minimum or maximum retention guardrails defined in bucket or IAM policies.
Do not configure Default Event Hold Duration because it is not relevant to fixed retention.

For more details, see Appendix A.1, Guidance for Fixed Retention Controls.
When a version is initially stored using these configured defaults for fixed retention:

The version's Object Lock Mode is set to the default value.
The Default Retention Period, (e.g., 6 Years), is added to the creation/storage timestamp to set the version's Retain Until Date.

For more details on fixed retention, see Appendix A.1, Guidance for Fixed Retention Controls.
</td></tr>
<tr><th>Variable retention (Configure bucket defaults for Object Lock Mode, Event Hold Duration and Retention Period)</th></tr>
<tr><td>

Configure the following bucket defaults for buckets that will store records requiring a variable retention period (e.g., Termination + 6 Years).

Configure Default Object Lock Mode to either Compliance (highly restrictive) or Governance (less restrictive).
Configure the Default Event Hold Duration to a value between 1 day and 100 years that satisfies any applicable minimum or maximum retention guardrails defined in bucket or IAM policies.

Cohasset asserts this should be configured to the post-event retention requirement, when it is practical to transition the Event Hold from On to Off soon after the business event occurs. If the transition will be performed long after the business event occurs, this default may be configured to a shorter period. See Appendix A.2, Guidance for Variable Retention Controls, examples C and D respectively.
Note: Event Hold is not a separate bucket default configuration. However, when bucket defaults are applied to a new record, storing a Default Event Hold Duration as version metadata will also store Event Hold set to On.

Configure the optional Default Retention Period to a value between 1 day and 100 years. When configured, this Default Retention Period must be (a) greater than or equal to the Event Hold Duration and (b) satisfy any applicable minimum or maximum retention guardrails defined in bucket or IAM policies.

While this is an optional configuration, Cohasset asserts this should always be configured to the shortest retention requirement for the record. This ensures that the version's initial Retain Until Date is set to the shortest time that the record must be kept, e.g., 6 Years for a retention period of Termination + 6 Years, and applies strong controls to prevent alteration, replacement, or deletion. See Appendix A.2, Guidance for Variable Retention Controls.

</td></tr>
</table>
</td></tr>
</table>

	Bucket, IAM Policy and Lifecycle Policy Configurations related to S3 Object Lock
	● When a version is initially stored using the configured defaults for variable retention: ○ The version's **Object Lock Mode** is set to the default value. ○ The version's **Event Hold** is set to On. ○ The version's **Event Hold Duration** is set to the default value. ○ The version's initial **Retain Until Date** is set as follows: ▪ If the optional **Default Retention Period** is configured, it is added to the creation/storage timestamp and stored as the version's initial **Retain Until Date**. ▪ Otherwise, the **Default Event Hold Duration** is added to the creation/storage timestamp and stored as the version's initial **Retain Until Date**. ● After the business event occurs (e.g., after termination), the record's **Event Hold** transitions from On to Off. During the transition, the record's currently stored **Event Hold Duration** is added to Current Time and this value is stored as the new **Retain Until Date**, if it is longer than the version's current **Retain Until Date**. ● For more details on variable retention, see Appendix A.2, *Guidance for Variable Retention Controls*. ● Authorized users may change the bucket default retention configurations at any time. The updated default values apply only to new versions and do not affect previously stored records; therefore, retention protections previously applied to an object version remain unchanged. ● For additional information, see Section 2.2.3.3, *Record Definition and Object Lock Controls*, which details the retention controls associated with each mode, and Appendix A, *Guidance for Applying Object Lock Controls*.
S3 bucket and IAM policy conditions (i.e., restrictions)	● Amazon S3 bucket policies and IAM policies may be used to restrict access to Amazon S3 resources and allow or deny operations. These policy conditions are evaluated when Object Lock values are transmitted, applied, or updated. An operation succeeds only when it satisfies all applicable bucket and IAM policy requirements. ○ Bucket policies are resource-based policies that apply to a bucket and the objects within that bucket. ○ IAM policies are identity-based policies that apply to operations issued by assigned users, groups, and roles. ● The following conditions pertain to Object Lock operations, and the operation succeeds only when it satisfies all applicable policy requirements; if either the bucket policy or the applicable IAM policy denies the operation, and it fails: ○ **s3:object-lock-mode:** Restricts the Object Lock Mode (i.e., Compliance and/or Governance). ○ **s3:object-lock-retain-until-date**: Restricts the Retain Until Date using a timestamp-based condition to enforce minimum and/or maximum retention expiration dates (Min/Max range specified as a timestamp). ○ **s3:object-lock-remaining-retention-days:** Restricts the retention period using a number of remaining retention days condition to enforce minimum and/or maximum retention dates (Min/Max range specified in days). ○ **s3:object-lock-event-hold-duration-days:** Restricts the Event Hold Duration using a number of days to enforce minimum and/or maximum allowable Event Hold Durations. ○ **s3:object-lock-event-hold:** Restricts the Event Hold status (i.e., On or Off). ○ **s3:object-lock-legal-hold:** Restricts the Legal Hold status (i.e., On or Off). ● Authorized users may change bucket and IAM policies, including the associated condition keys. ○ The condition keys that are in effect when an operation is issued are evaluated as part of the policy decision to allow or deny that operation. ○ Policy changes do not change Object Lock values already stored with existing object versions. ● For additional information on S3 Object Lock-related condition keys, see Appendix A.3, *Condition Keys for Bucket and IAM Policies*.

	Bucket, IAM Policy and Lifecycle Policy Configurations related to S3 Object Lock
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 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 versions stored in the bucket.

2.2.3.3 Record Definition and Object Lock Controls

- Each object version is managed as a separate record, with its own Object Lock retention control metadata and Legal Hold status. Each record (i.e., object version) is comprised of:
  - The complete content of the object version, which is unmodifiable.
  - Immutable metadata, which includes, but is not limited to, unique Object Key Name, version identifier, creation/storage timestamp (*lastmodified* timestamp), object size, and user-defined metadata (name-value pairs).
  - Mutable metadata, which includes, but is not limited to, Object Lock controls (Retain Until Date, Object Lock Mode, Event Hold, Event Hold Duration, and Legal Hold), Amazon S3 Access Control Lists (ACLs), and Amazon S3 tags.
  - Annotations, which cannot be created, updated or deleted for the versions after Object Lock retention controls are applied in either Compliance or Governance modes. Users with *BypassGovernanceRetention* permission cannot override the restrictions on annotation operations.
- An assortment of retention controls is allowed within a single bucket. For example, a bucket with the Object Lock feature enabled may contain versions with fixed and variable retention applied in either Compliance or Governance mode, as well as versions without retention protection. Additionally, a Legal Hold status of On or Off may be applied to object versions, independent of retention controls.
- Object Lock controls may be applied and/or changed on (a) individual object versions, via REST APIs (Application Programming Interface), AWS CLI (Command Line Interface), SDKs (Software Development Kits), or the Amazon S3 console or (b) many object versions at once, via S3 Batch operations. This assessment report describes operations as REST APIs.
- The following two subsections describe methods of applying and updating fixed and variable retention. The third subsection describes the controls applied by Object Lock retention. Also, see Appendix A, *Guidance for Applying Object Lock Controls*.

2.2.3.3.1 Applying **Fixed** Retention Controls

- Fixed retention controls, when applied in either Compliance or Governance mode, protect an object version for a fixed contiguous period of time, (i.e., until the record's Retain Until Date expires).

- The following table summarizes the process of applying **fixed retention** during object creation operations (i.e., PutObject, CopyObject, or CreateMultipartUpload). The left column describes the criteria when the object is being written, the validations that must be passed (center column) and the Object Lock metadata applied to the object version (right column), which assumes that the validations passed. If any validation does not pass, the write operation fails and the object version is not stored.

Fixed Retention Criteria at Write	Validations	Retention metadata applied to the object version, when Validations are passed
1. Object Lock Mode and Retain Until Date are explicitly transmitted (whether or not bucket defaults are configured).	• Is the transmitted Object Lock Mode Compliance or Governance, and • Is the transmitted Retain Until Date in the future, and • Do the transmitted Object Lock parameters satisfy all applicable bucket and IAM policy conditions?	• The object version is stored with two Object Lock retention values: ○ Object Lock Mode, as transmitted, and ○ Retain Until Date, as transmitted. • Any configured bucket defaults are not applied to the object version.
2. Only Legal Hold is explicitly transmitted (whether or not bucket defaults are configured).	• Is the transmitted Legal Hold status valid (i.e., is the status On or Off), and • Does the transmitted Legal Hold status satisfy applicable bucket and IAM policy conditions?	• The object version is stored with the transmitted Legal Hold status (On or Off). • Any configured bucket defaults are not applied to the object version.
3. Object Lock Mode, Retain Until Date and optional Legal Hold are explicitly transmitted (whether or not bucket defaults are configured).	• Validations for Object Lock fixed retention must pass (see row #1), and • Validations for Legal Hold, if explicitly transmitted, must pass (see row #2).	• The object version is stored with the Object Lock retention values, as described in row #1, and the Legal Hold status (On or Off), if explicitly transmitted. • Any configured bucket defaults are not applied to the object version.
4. Retention metadata and Legal Hold status are not transmitted, and bucket defaults are configured for fixed retention (i.e., Object Lock Mode and Retention Period are configured as bucket defaults).[15]	• Do existing bucket default values, when applied to an object, satisfy applicable bucket and IAM policy conditions?	• The object version is stored with bucket default Object Lock retention values: ○ Object Lock Mode, and ○ Retain Until Date, calculated as the version's creation/storage timestamp plus bucket's Default Retention Period. • Note: S3 does not currently offer bucket default Legal Hold status; thus, Legal Hold will not be set.
5. No retention metadata is explicitly transmitted and bucket defaults are not configured. Transmission of Legal Hold status (On/Off) is optional.	• Validations for Legal Hold, if explicitly transmitted, must pass (see row #2).	• The object version is stored without retention controls. • The Legal Hold status is stored, if transmitted.

[15] See the row entitled *Default retention configurations* in Section 2.2.3.2, *Amazon S3 Immutability and Retention Configurations*, for Cohasset's recommendations for bucket default configurations.

- In addition to applying fixed retention controls during the initial storage process, explicit retention controls may be applied or changed on an existing object version using the PutObjectRetention API, as described in the following table. The updated retention controls are applied to the explicit object version if the version identifier is specified, otherwise, the updated retention controls are applied to the current (top) object version.

Fixed Retention Change	Validations	Retention metadata applied to the object version, if Validations are passed
1. Set or change fixed retention values, without using *BypassGovernance-Retention.*	• Is the transmitted Object Lock Mode (Compliance or Governance) the same as the version's currently stored mode, and • Is the transmitted Retain Until Date: ○ A date in the future, and ○ Greater than or equal to the version's currently stored Retain Until Date, and • Do the transmitted Object Lock parameters satisfy all applicable bucket and IAM policy conditions?	• The version is updated with the Object Lock Mode and Retain Until Date, as transmitted. • The version's Event Hold status is set to Off, if transmitted.
2. Change fixed retention values, using *BypassGovernance-Retention.*	• Is the version's currently stored Object Lock Mode Governance, and • Are the requirements[16] for the privileged change that requires *BypassGovernanceRetention* met, and • Do the transmitted Object Lock parameters satisfy all applicable bucket and IAM policy conditions?	• The version is updated with the Object Lock Mode and Retain Until Date, as transmitted. • The version's Event Hold status is set to Off, if transmitted.
3. Remove Governance mode retention, using *BypassGovernance-Retention.*	• Is the version's currently stored Object Lock Mode Governance, and • Does the user have *BypassGovernanceRetention* permissions and is x-amz-bypass-governance-retention in the header, and • Are transmitted retention values empty to remove retention controls, and • Do bucket and IAM policy conditions allow for the transmission of empty retention values?	• Governance mode Object Lock retention controls are removed from the version.

2.2.3.3.2 Applying **Variable** Retention Controls

- Variable retention controls, when applied in either Compliance or Governance mode, protect an object version for an indefinite period of time, until a business event (e.g., contract completion, account closure, claim resolution) occurs.
  - When variable retention controls are applied to an object version, an initial Retain Until Date is stored as version metadata. The Retain Until Date is set to (a) a future date explicitly transmitted with the object version, or (b) dynamically calculated by adding the version's transmitted Event Hold Duration to the creation/storage timestamp, or (c) calculated using bucket defaults if no explicit retention values are

[16] Requirements for *BypassGovernanceRetention* include: (a) the user has *BypassGovernanceRetention* permission, (b) x-amz-bypass-governance-retention is in the header, and (c) valid Object Lock Mode and Retain Until Date values are transmitted.

transmitted with the version. This initial Retain Until Date may be extended anytime, using the PutObjectRetention API, but cannot be reduced unless overriding Governance mode retention controls.

- While the Event Hold is active (set to On), the object version is retained indefinitely and S3 dynamically calculates a Retain Until Date during every read operation (e.g., GetObjectRetention, HeadObject, GetObject) and displays the greater of (a) the Event Hold Duration value plus Current Time or (b) the version's currently stored Retain Until Date. This displayed date represents the earliest date the object version is eligible for deletion if the Event Hold were immediately cleared (set to Off).
  - The Event Hold Duration value may be increased or decreased while the Event Hold is active (On). When the Event Hold Duration is changed, S3 recalculates the Retain Until Date using the *greater* of the previous and updated Event Hold Duration values added to the Current Time. The currently stored Retain Until Date metadata is updated only when the recalculated Retain Until Date exceeds the currently stored Retain Until Date.
- Once the business event occurs, variable retention is transitioned to fixed retention by setting the Event Hold to Off. As part of this process, the version's currently stored Retain Until Date is updated if (a) the version's Event Hold Duration plus Current Time is greater than the version's currently stored Retain Until Date or (b) the operation specifies a future Retain Until Date that is greater than the calculated Retain Until Date.

► The following table summarizes the process of applying **variable retention** during object creation operations (i.e., PutObject, CopyObject, or CreateMultipartUpload). *This table assumes that Event Hold is set to On to initiate the indefinite period for variable retention*. The left column describes the criteria when the object is being written, the validations that must be passed (center column) and the Object Lock metadata applied to the object version (right column), which assumes that the validations passed. If any validation does not pass, the write operation fails and the object version is not stored.

Variable Retention Criteria at Write	Validations	Retention parameters stored for the object version, if Validations are passed
1. Object Lock Mode, Event Hold set to On and Event Hold Duration, along with an optional Retain Until Date, are explicitly transmitted (whether or not bucket defaults are configured).	• Is the transmitted Object Lock Mode Compliance or Governance, and • Is the transmitted Event Hold valid (i.e., On), as required for variable retention, and • If the optional Retain Until Date is transmitted, is it in the future, and is it equal to or greater than the calculated Retain Until Date (i.e., Event Hold Duration added to creation/storage timestamp), and • Do the transmitted Object Lock parameters satisfy all applicable bucket and IAM policy conditions?	• The object version is stored with four Object Lock retention values: ○ Object Lock Mode, as transmitted, and ○ Event Hold status transmitted as On, and ○ Event Hold Duration, as transmitted, and ○ Retain Until Date, as transmitted, or if this value is not transmitted, a dynamically calculated value is stored by adding the Event Hold Duration to the creation/storage timestamp. • Any configured bucket defaults are not applied to the object version.
2. Only Legal Hold is explicitly transmitted (whether or not bucket defaults are configured).	• Is the transmitted Legal Hold status valid (i.e., is the status On or Off), and • Does the transmitted Legal Hold status satisfy applicable bucket and IAM policy conditions?	• The object version is stored with the transmitted Legal Hold status (On or Off). • Any configured bucket defaults are not applied to the object version.

Variable Retention Criteria at Write	Validations	Retention parameters stored for the object version, if Validations are passed
3. Object Lock Mode, Event Hold and Event Hold Duration, along with an optional Retain Until Date, and optional Legal Hold are explicitly transmitted (whether or not bucket defaults are configured).	• Validations for Object Lock variable retention must pass (see row #1), and • Validations for Legal Hold, if explicitly transmitted, must pass (see row #2).	• The object version is stored with the Object Lock retention values, as described in row #1, and the Legal Hold status (On or Off), if explicitly transmitted. • Any configured bucket defaults are not applied to the object version.
4. Retention metadata and Legal Hold status are not transmitted, and bucket defaults are configured for variable retention (i.e., Object Lock Mode, Event Hold set to On, Event Hold Duration and optional Retention Period are configured as bucket defaults).[17]	• Do existing bucket default values, when applied to an object, satisfy applicable bucket and IAM policy conditions?	• The object version is stored using the bucket default Object Lock retention values: ○ Object Lock Mode, ○ Event Hold (must be On for variable retention), ○ Event Hold Duration, and ○ Retain Until Date, calculated as follows: ▪ If the optional Default Retention Period is set, it is added to the creation/storage timestamp. ▪ Otherwise, the Default Event Hold Duration is added to the creation/storage timestamp. • Note: S3 does not currently offer bucket default Legal Hold status; thus, Legal Hold will not be set.
5. No retention metadata is explicitly transmitted, and bucket defaults are not configured. Transmission of Legal Hold (On/Off) is optional.	• Validations for Legal Hold, if explicitly transmitted, must pass (see row #2).	• The object version is stored without retention controls. • The Legal Hold status is stored, if transmitted.

- The following table describes how explicit retention controls are applied or changed on an existing object version using the PutObjectRetention API.
  - The first row of the following table explains the PutObjectRetention API used to clear the Event Hold (Off) and set the final Retain Until Date. For example, if the variable retention is Termination +6 Years, the Event Hold would be cleared after the termination occurred, and the final Retain Until Date would be set to 6 years following the termination date.
- The updated retention controls are applied to the explicit object version if the version identifier is specified, otherwise, the updated retention controls are applied to the current (top) object version.

[17] See the row entitled *Default retention configurations* in Section 2.2.3.2, *Amazon S3 Immutability and Retention Configurations*, and Appendix A, *Guidance for Applying Object Lock Controls*, for Cohasset's recommendations for bucket default configurations.

Variable Retention Change	Validations	Retention metadata applied to the object version, if Validations are passed

1. Clear Event Hold (set to Off), and optionally change retention values, without using *BypassGovernance-Retention.*	• Is the transmitted Object Lock Mode (Compliance or Governance) the same as the version's currently stored mode, and
	• Is Event Hold transmitted as Off (assumed for this row), and
	• Is Event Hold Duration not transmitted? (Event Hold Duration is disallowed when transmitting Event Hold=Off)
	• If the optional Retain Until Date is transmitted, is it:
	  ○ A date in the future, and
	  ○ Greater than or equal to the dynamically calculated Retain Until Date, and
	  ○ Greater than or equal to the currently stored Retain Until Date, and
	• Do the transmitted Object Lock parameters satisfy all applicable bucket and IAM policy conditions?
		• Object Lock Mode, as transmitted.
		• Event Hold=Off, as transmitted.
		• Retain Until Date, as transmitted, or if none is transmitted, the dynamically calculated Retain Until Date is stored if it is greater than or equal to the currently stored Retain Until Date.
		• Note: Changing Event Hold to Off transitions the record from variable to fixed retention.

2. Set or change variable retention values, assume transmitting Event Hold=On (regardless of the version's currently stored Event Hold value), without using *BypassGovernance-Retention.*	• Is the transmitted Object Lock Mode (Compliance or Governance) the same as the version's currently stored mode, and
	• Is Event Hold transmitted as On (On is assumed for this row), and
	• Is the transmitted Event Hold Duration valid (between 1 day and 100 years), and
	• If the optional Retain Until Date is transmitted, is it:
	  ○ A date in the future, and
	  ○ Greater than or equal to the dynamically calculated Retain Until Date, and
	  ○ Greater than or equal to the version's currently stored Retain Until Date, and
	• Do the transmitted Object Lock parameters satisfy all applicable bucket and IAM policy conditions?
		• Object Lock Mode, as transmitted.
		• Event Hold = On, as transmitted.
		• Event Hold Duration, as transmitted.
		• Retain Until Date, as transmitted, or if this value is not transmitted, S3 recalculates the Retain Until Date by adding the *greater* of the previous and updated Event Hold Duration to the Current Time. If this calculated Retain Until Date is greater than the version's currently stored Retain Until Date, the calculated date is stored; otherwise, the Retain Until Date is not updated.

3. Change variable retention values, using *BypassGovernance-Retention.*	• Is the version's currently stored Object Lock Mode Governance, and • Are the requirements[18] for the privileged change that requires *BypassGovernanceRetention* met, and • Do the transmitted Object Lock parameters satisfy all applicable bucket and IAM policy conditions?	• The version is updated with the Object Lock retention controls, as transmitted.
4. Remove Governance mode retention, using *BypassGovernance-Retention.*	• Is the version's currently stored Object Lock Mode Governance, and • Does the user have *BypassGovernanceRetention* permissions and is *x-amz-bypass-governance-retention* in the header, and • Are transmitted retention values empty to remove retention controls, and • Do bucket and IAM policy conditions allow for the transmission of empty retention values?	• Governance mode Object Lock retention is removed from the version.

[18] Requirements for *BypassGovernanceRetention* include: (a) the user has *BypassGovernanceRetention* permission, (b) x-amz-bypass-governance-retention is in the header, and (c) valid Object Lock Mode and Retain Until Date values are transmitted.

- Once an Event Hold is cleared (Off), continued retention of the record is governed by fixed retention controls (i.e., the applied Object Lock Mode and Retain Until Date). A dynamically calculated Retain Until Date is no longer created during each read operation.

2.2.3.3.3 Object Lock 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**
Uniquely identifying records and protecting immutable attributes	● Each record in Amazon S3 is assigned a unique identifier, which facilitates findability. Specifically, Amazon S3 captures the following metadata for each 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. Notes: By default, Amazon S3 general purpose bucket names must be unique across all AWS accounts and all AWS Regions within an AWS partition. Amazon S3 also supports account regional namespaces, in which bucket names must be unique within the account regional namespace rather than the shared global namespace. 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.	
Managing versions, and protecting record content and immutable metadata	● Versioning must be enabled on a bucket with Object Lock. When enabled, each version of an object is considered a separate record and must have its own applied retention and Legal Hold values. ● Each version, together with its immutable 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 and Legal Hold values. ○ 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 must be created. ○ If the Object Lock Mode, Retain Until Date, Event Hold, Event Hold Duration, Legal Hold, 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 cleared (Off), the version may be deleted but cannot be modified or overwritten.	
Restricting changes to applied retention controls	● The Object Lock feature applied to a bucket cannot be removed. ● For versions set to Compliance mode, authorized users and/or Lifecycle policies: ○ Cannot downgrade the Object Lock Mode from Compliance to Governance or remove the Object Lock Compliance mode. ○ Can enable (On) or clear (Off) an Event Hold. ○ Can extend or reduce the Event Hold Duration for active Event Holds. ○ Can extend the Retain Until Date. ○ Cannot reduce the Retain Until Date.	● For versions in Governance mode, users without the *BypassGovernanceRetention* permission are subject to the same controls as in Compliance mode. ● Further, users with *BypassGovernanceRetention* permissions may: ○ Change Object Lock Mode from Governance to Compliance and update the Retain Until Date. ○ Reduce the Retain Until Date. ○ Remove the Object Lock Governance mode and the retention controls, entirely.

	Object Lock, in highly restrictive Compliance mode	Object Lock, in less restrictive Governance mode
	Accordingly, Compliance mode ensures that Object Lock retention controls are not circumvented by any user or process.	Accordingly, procedural controls and monitoring are required to scrutinize privileged administrator actions taken to change or remove Object Lock retention controls.
Applying and clearing legal holds	• A Legal Hold may be enabled (On) which prevents the overwrite or deletion of that object version until the Legal Hold is cleared (Off). ○ The Legal Hold attribute may be enabled regardless of an object version's Object Lock status. ○ Using *BypassGovernanceRetention* does not ignore (bypass) an object's legal hold status; if a version's Legal Hold is set (On), attempts to delete the version are prohibited. • See Section 2.2.3.4, *Legal Holds (Temporary Holds)*.	
Restricting deletion of records and buckets	• Deleting a specific version is allowed only when the version's: ○ Retain Until Date is expired, ○ Event Hold is cleared (Off) or not set, and ○ Legal Hold is cleared (Off) or not set. Compliance mode ensures that Object Lock retention controls are not circumvented by any user or process.	• The controls described for Compliance mode apply to users without *BypassGovernanceRetention* permission. • Users with *BypassGovernanceRetention* permission may delete a version with unexpired retention controls, if the version's Legal Hold status is Off or not set. Accordingly, procedural controls and monitoring are required to scrutinize privileged administrator actions to prematurely delete versions.
	• Deleting an object (without identifying the version) appends a delete marker as the current (top) version and all other existing versions are hidden but remain unmodifiable. The Delete marker may be removed to reinstate the original 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 Object Lock retention and Legal Hold metadata. The original record and its metadata 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 changed, 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 cleared.

- 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).
- The Legal Hold status is independent of the version's retention controls; therefore, a Legal Hold status may be applied to a version without applied retention controls.
- The Legal Hold status must be separately set for each object version. When the Legal Hold status is enabled (On), it prohibits deleting the object version, and when cleared (Off) or not set, preservation is not mandated; however other retention controls (if any) continue to apply.

- Note: Explicitly transmitting Legal Hold for an object overrides bucket default retention configurations. Therefore, if an object is transmitted with a Legal Hold status (On or Off), the object does not inherit the bucket's default Object Lock retention configurations (if any).

- The *BypassGovernanceRetention* permission does not circumvent a version's Legal Hold status. If a version's Legal Hold status is set (On), attempts to delete the 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) (b) the Event Hold attribute is cleared (Off) or is not set, and (c) its Legal Hold attribute is cleared (Off) or not set.
  - Eligibility for deletion does not result in automatic deletion.
- The following table summarizes actions taken to delete 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, with a unique version identifier, is added as the current (top) version, whether or not the object is eligible for deletion.
	  ○ The delete marker hides the other versions of the object.
	  ○ The delete marker does not affect the content or metadata associated with the other versions of the object.
	• Delete markers can be removed, which results in reinstating (i.e., unhiding) the other versions of the object.
	• A Lifecycle policy may be configured to issue delete operations 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 as the current (top) version, whether or not the object is eligible for deletion.
	  ○ If the current version is a delete marker and one or more older (hidden) 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., there are no older (hidden) versions), 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 retention and Legal Hold controls apply, and only eligible versions are deleted. ○ An error is logged, and the operation is rejected if the user does not have the required permissions or the user attempts to delete an object version that is not eligible. • A Lifecycle policy may be configured to automatically delete object versions. Only object versions that are eligible for deletion are permanently deleted.	
	• *BypassGovernanceRetention* (i.e., privileged delete) is not available to any administrator or user to prematurely delete object versions. Accordingly, Compliance mode ensures that Object Lock retention controls are not circumvented by any user or process.	• The *BypassGovernanceRetention* permission cannot be utilized with a Lifecycle policy. • However, users with *BypassGovernanceRetention* permission may delete an unexpired object version, if the version's Legal Hold status is Off or not set. 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 Transport Layer Security (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. SSE-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 Key Management System (KMS) 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 operation 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 Access Control (RBAC) is employed by AWS. The permissions for each user are controlled through IAM roles created for the client organization.
- Condition keys can be set in bucket and IAM policies to impose additional restrictions on object-level operations.
  - Bucket policies are resource-based and apply restrictions to the bucket and the object versions within the bucket.
  - IAM policies are identity-based and apply restrictions to operations issued by users, groups, and roles.

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 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:

- Properly configuring buckets intended to store required records by enabling versioning and the Object Lock feature, which allows Object Lock retention controls to be applied to stored records.
- Configuring bucket and IAM policies with appropriate condition keys to impose additional restrictions on object-level operations.
- Assigning appropriate permissions for managing retention controls and properly configuring the Identity and Access Management (IAM) roles.
- Ensuring all required records are stored with integrated retention controls, preferably within 24 hours of creation, by (a) configuring Object Lock retention defaults and transmitting new versions without any retention and Legal Hold values, so the bucket default values are applied or (b) transmitting unique retention and Legal Hold values with each version. Note: Care must be taken, since transmitting a Legal Hold status of On or Off overrides bucket default retention settings.
  - For fixed retention, apply an appropriate Object Lock Mode and Default Retention Period for each required record (i.e., each object version).
  - For variable retention, apply an appropriate Object Lock Mode, Event Hold attribute set to On, Event Hold Duration and Retain Until Date that meets or exceeds the post-event retention requirement for each record (i.e., each object version).
  - See Section 2.2.3, *Amazon S3 Capabilities*, and Appendix A, *Guidance for Applying Object Lock Controls*, for additional information.
- Monitoring variable retention to ensure (a) Event Holds are released after the business event occurs, and (b) the final Retain Until Date is set to a value that meets the record's full retention requirement.
- 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 who can remove or reduce less-restrictive Governance retention controls, and regularly monitor privileged administrative actions.
- Limiting the creation and management of delete markers. Specifically, Cohasset recommends always specifying the version identifier in delete operations.

- 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.

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[19] until the applied retention controls and Legal Holds have expired 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 and use the records.

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 additional 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.

[19] 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.

- 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 requests the checksum for the object and uses 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 additional 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 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: By default, Amazon S3 general purpose bucket names must be unique across all AWS accounts and all AWS Regions within an AWS partition. Amazon S3 also supports account regional namespaces, in which bucket names must be unique within the account regional namespace rather than the shared global namespace.
  - A **version identifier**, which is automatically assigned to each new version of the object.
  - The creation/storage timestamp, which is system-generated. Note: For large objects transmitted using the CreateMultipartUpload API, the creation/storage timestamp is captured at the start of the upload process.
- Amazon ensures 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:
  - View retention controls for each object version by selecting the version switch in the S3 Console.
  - Generate scheduled inventory reports for a specific bucket or for objects that share a common prefix. Selection criteria may include metadata applied to each object version, including Object Lock Mode, Retain Until Date, Event Hold status, Event Hold Duration, and Legal Hold status.
  - 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 operations:
    - **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. Note: Object Lock metadata is not included with the list of objects.
    - **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. Note: Object Lock metadata is not included with the list of objects.
    - **HeadObject and GetObjectRetention**: Returns the object metadata, including retention settings for the current (top) version, without returning the object itself. For records under variable retention, the Object Lock Mode, current dynamically calculated Retain Until Date, Event Hold attribute status (On/Off), and Event Hold Duration are included.
  - Get objects using the GetObject operation:
    - When the operation 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, based on the user's permissions, 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 operations.

Note: For each of the above actions, certain metadata (e.g., Object Key Name, version identifier, creation/storage timestamp, Object Lock retention values, and Legal Hold status) will be returned for each object, based on the user's permissions. For example, an active Legal Hold value is only returned if the user has permission to view an object's legal hold status.

2.4.4 Additional Considerations

In addition, 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

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 adopted two redundancy options, paragraphs (A) or (B).

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 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.[20] [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.[21] [emphasis added]

[20] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66421.

[21] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66421.

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 additional 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. The CRR configuration may apply to an entire bucket or to select criteria, (e.g., Object Key Name prefix or Amazon S3 tags) that 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, Event Hold, Event Hold Duration, and Legal Hold status) applied to object versions 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, Event Hold, Event Hold Duration, 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, an Event Hold Duration is modified, an Event Hold is cleared, 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, Immutability and Retention Controls*, for a description of allowed changes to retention controls for objects with an Object Lock Mode set to Compliance or Governance.)
    - Notes:
      - Retention settings updated on the target bucket do not synchronize to the source bucket. Therefore, to ensure the same settings for both buckets, Cohasset recommends all retention control changes be made to objects in the source bucket, for automatic synchronization to the target bucket.
      - When an Event Hold is cleared on the source, S3 replicates the change to the target bucket, and the target environment calculates its own final Retain Until Date based on the time of replication. For predictable replication timing, S3 Replication Time Control is recommended.

- 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 11-nines durability of stored data 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: By default, Amazon S3 general purpose bucket names must be unique across all AWS accounts and all AWS Regions within an AWS partition. Amazon S3 also supports account regional namespaces, in which bucket names must be unique within the account regional namespace rather than the shared global namespace.
  - 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 users 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 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 *BypassGovernanceRetention* permission.
    - Management event history is viewable with limited search and filter options via the CloudTrail console or via API and CLI operations.
  - 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, using PutObjectRetention operations to add or change variable retention controls, applying a legal hold, and deleting an object.
    - Data events may be queried via API or CLI operations; 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).

In the May 30, 2017, adopting release, the CFTC amended its recordkeeping obligations to *"modernize and make technology neutral the form and manner in which regulatory records must be kept"*. The CFTC amendments replaced previous requirements to retain records in a non-rewriteable, non-erasable record format (a.k.a., WORM) with a less-prescriptive, principles-based approach to recordkeeping.

> *Consistent with the Commission's emphasis on a less-prescriptive, principles-based approach, [the final rule] 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.*[22] [emphasis added]

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 for electronic recordkeeping, (i.e., (a) record and complete time-stamped audit trail and (b) 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.*[23] [emphasis added]

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), including requirements for non-rewriteable, non-erasable record format. Specifically, Cohasset assesses Amazon S3 with the Object Lock feature applied in either:

- Compliance mode, a highly restrictive option that applies integrated controls to protect against overwrites and modifications and enforces strict retention controls, or

[22] 2017 CFTC Recordkeeping Requirements Adopting Release, 82 FR 24482.

[23] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.

- Governance mode, a less restrictive option that protects against overwrites and modifications but requires administrative procedures and monitoring to ensure compliant retention, since privileged administrators are allowed to reduce or remove retention controls.

See Section 2.2, *Non-Rewriteable, Non-Erasable Record Format*, for information on the Object Lock controls.

In the following table, Cohasset correlates the specific *principles-based* CFTC requirements for electronic records with the assessed functionality of Amazon S3 when the Object Lock feature is properly configured and applied to meet SEC requirements. The first column enumerates requirements of the CFTC regulation. The second column provides Cohasset's analysis and opinion regarding the capabilities of S3, relative to these requirements.

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[24] with fixed and variable retention periods, are met by the functionality of Amazon S3, with the Object Lock feature applied in either Compliance or Governance mode. 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, Event Hold Duration) and legal hold attributes. The most recent values of mutable metadata are retained for the same time period as the associated records.

[24] 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)**
	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;	It is Cohasset's opinion that Amazon S3 capabilities described in Section 2.5, *Record Redundancy*, including methods for a persistent duplicate copy or 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*.
(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[25] 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 both fixed and variable retention periods, when the Object Lock feature is properly applied in either Compliance or Governance mode.
- Allows a Legal Hold status to be set to On for objects subject to preservation requirements, which retains (preserves) the object as immutable and prohibits deletion or overwrites until the Legal Hold status is cleared.
- Prohibits deletion of a record and its immutable metadata by standard users until the applied Retain Until Date has expired, any Event Hold is cleared, and the Legal Hold status is cleared, though privileged users may prematurely delete versions with less-restrictive Governance retention controls.
- 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 TLS (Transport Layer Security) or by client-side encryption.
- Verifies the accuracy and quality of the recording process by requiring the source system to provide a checksum that is used both during the initial write operation and during subsequent post-recording verification operations.
- Allows authorized users to access 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-Region 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).

[25] 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 • Guidance for Applying Object Lock Controls

Section 2, *Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e)*, and Appendix B, *Overview of Relevant Electronic Records Requirements*, describe the stringent electronic recordkeeping system requirements applicable to broker-dealers. In addition, in the 2001 Transfer Agent Recordkeeping Requirements Adopting Release, the SEC indicated that more stringent record preservation controls are warranted for broker-dealer records because of the greater risks associated with potential record alteration and engagement in activities involving customer funds, accounts, and securities transactions:

> *The Commission believes that using a set of requirements to ensure security and integrity of records is appropriate in the transfer agent context, unlike the broker-dealer context, because of the lower risks from record alteration for transfer agents. There appear to be a lower incidence of altered transfer agent records and the Commission staff has brought few enforcement actions against transfer agents based on alteration of their records. In addition, transfer agents do not hold customer funds, open accounts, or recommend investments. Therefore, the Commission generally does not inspect transfer agents for financial and sales practice problems.* ***** [26] [emphasis added]

Considering these SEC statements, the examples in Appendix A.1, *Guidance for Fixed Retention Controls*, and A.2, *Guidance for Variable Retention Controls*, describe retention configuration options that Cohasset asserts are consistent with SEC Rules 17a-4(f) and 18a-6(e). In addition, Cohasset describes one variable retention configuration that it asserts should not be used for required records.

A.1 Guidance for Fixed Retention Controls

By definition, fixed retention periods require keeping records for a set period (e.g., 6 Years) starting from the creation/storage timestamp. Business need or regulatory amendment may require future changes to the retention period.

With fixed retention, the following retention values are stored as version metadata to prevent deletion:

1. The **Object Lock Mode** of Compliance (highly restrictive) or Governance (less restrictive).
2. The **Retain Until Date**, which Cohasset strongly recommends setting to the full retention requirement during record creation or within 24 hours to prevent alteration, replacement, or deletion before the Retain Until Date expires.
   - When the Object Lock Mode is set to Compliance, S3 ensures that the version's Retain Until Date cannot be reduced by any user, and no user can prematurely delete the version.
   - When the Object Lock Mode is set to Governance, S3 ensures that only privileged users (i.e., users with *BypassGovernanceRetention* permission) can reduce the Retain Until Date or prematurely delete the version.

[26] Recordkeeping Requirements for Transfer Agents, Exchange Act Release No. 34-44227, 66 FR 21650-51 (May 1, 2001).

Retention controls are applied to record versions during creation by either:

1. **Configuring and Relying on Bucket Defaults for Fixed Retention** and not transmitting specific Object Lock retention or Legal Hold values with the object when bucket defaults are being applied, or
2. **Explicitly Transmitting Fixed Retention with the Object** and not relying on bucket default retention values. Reminder: Transmitting explicit Object Lock values with the object overrides any bucket defaults.

Each approach is described in the following subsections, with examples illustrating how retention is applied and managed. All examples assume that the *BypassGovernanceRetention* permission is not used.

A.1.1 Configuring and Relying on Bucket Defaults for Fixed Retention

Cohasset recommends configuring bucket defaults for Object Lock retention on all buckets that may store required records. These bucket defaults help ensure retention controls are applied consistently when records are stored, without requiring source systems to transmit explicit retention values with each record.

When bucket default retention configurations do not meet the full retention requirement for a particular record, the source system can transmit explicit Object Lock retention values with the object during storage, and these explicit values override the bucket defaults. For additional information, see Section A.1.2, *Explicitly Transmitting Fixed Retention with the Object*.

Cohasset has identified three different approaches to configuring bucket default retention:

1. **Least Restrictive Retention Controls:** Configure bucket defaults to meet the least restrictive retention requirements (e.g., shortest retention period) and transmit explicit Object Lock retention values for records requiring more restrictive or longer retention protections.
2. **Most Restrictive Retention Controls:** Configure bucket defaults to align with the most restrictive retention requirements (e.g., longest retention period). Then, transmit explicit Object Lock retention values for records requiring less restrictive or shorter retention protections.
3. **Most Common Retention Controls:** Configure bucket defaults to align with the most common retention requirements for records stored in the bucket. Then, transmit explicit Object Lock retention values only when different retention settings are needed.

The following table summarizes the bucket default configurations for fixed retention. The default values must satisfy the bucket and IAM policy conditions; see Appendix A.3, *Condition Keys for Bucket and IAM Policies*, for more information.

Default Parameter	Bucket default configurations for fixed retention
Default Object Lock Mode	● Configure this default to either highly restrictive **Compliance** mode or less restrictive **Governance** mode. ○ If configuring to less restrictive Governance mode, plan and implement procedural controls to monitor reductions to the Retain Until Dates and removal of Object Lock retention controls.

Default Parameter	Bucket default configurations for fixed retention
Default Retention Period	● Configure this default to the retention period, in days or years, based on the selected approach for configuring bucket defaults (e.g., least restrictive, most restrictive or most common). When the version is initially stored, the Default Retention Period is added to the version's creation/storage timestamp to calculate the initial Retain Until Date, which is stored with the object. Note: Amazon S3 supports fixed retention periods ranging from 1 day to 100 years. ○ If the regulated entity's internal retention standard is longer than the regulatory requirement, Cohasset recommends collaborating with the Compliance Officer and business operations to determine whether the Default Retention Period should be configured with the regulatory requirement or the entity's longer internal retention standard. ▪ **When Object Lock is applied in Compliance mode, a version's Retain Until Date cannot be reduced after it is applied**.
Default Event Hold Duration	● Do not configure this default because it pertains to variable retention. See Appendix A.2, *Guidance for Variable Retention Controls*.

When these defaults are applied to an object version during the storage process, the version's Object Lock Mode is set to the default value and the Default Retention Period, (e.g., 6 Years), is added to the creation/storage timestamp to set the version's Retain Until Date.

After the object is stored, its retention metadata can be updated without creating a new version:

- The Object Lock Mode is typically the same but may be more restrictive (i.e., changing from Governance to Compliance) though it cannot be downgraded from Compliance.
- The Retain Until Date may be extended at any time, whether the retention controls are set to Compliance or Governance mode, and privileged users may reduce the Retain Until Date for versions set to Governance mode.

Cohasset recommends setting the Legal Hold status only after the object is stored, as needed. Important Note: If a Legal Hold status (On or Off) is transmitted with the object during creation, the bucket defaults for Object Lock retention will not be applied to the object.

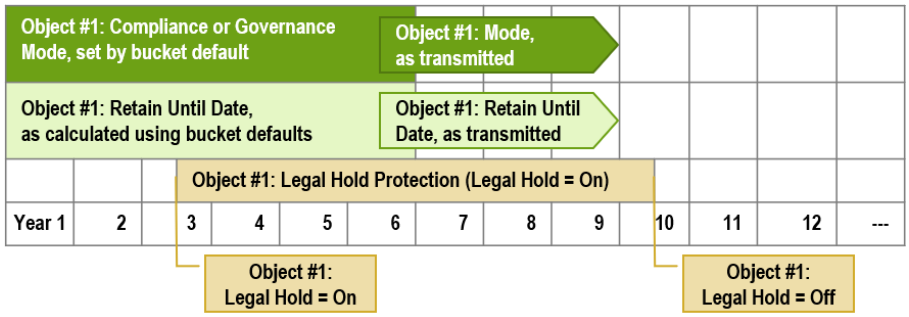
A.1.1.1 Example A: Fixed retention (bucket defaults applied), with retention extension and Legal Hold

Example A illustrates retention controls for a fixed retention period of 6 Years, when the following bucket defaults are configured as follows:

- **Bucket Default Object Lock Mode** is configured to Compliance or Governance.
- **Bucket Default Retention Period** is configured to 6 Years.
- **Bucket Default Event Hold Duration** is not configured because it is only relevant to variable retention, as described in Section A.2, *Guidance for Variable Retention Controls*.

These bucket defaults are used to store metadata for Object #1, which is a specific object version. Separately, the Legal Hold status is also set and cleared, which updates the version's metadata. The operations to manage the version's retention and Legal Hold values are described in the table below the illustration.

Example A: Fixed Retention (bucket defaults applied), with retention extension and Legal Hold



	Object Lock Mode	Retain Until Date	Legal Hold	Operations
Object #1 creation	Set the mode to the bucket default value	Set the timestamp, as **calculated** using bucket defaults	Not set	At creation, Object #1 is stored without transmitting explicit retention values or a Legal Hold status: ● The Object Lock Mode is stored by applying the bucket **Default Object Lock Mode**. ● The Retain Until Date is stored as 12/31 of year 6, by adding the bucket **Default Retention Period** (i.e., 6 Years) to the version's creation/storage timestamp. ● The version's Legal Hold status must not be set when applying bucket retention defaults.
Year 3 (6/30)	Not updated	Not updated	Set to On, as transmitted	On 6/30 of year 3, the version's Legal Hold status is set to On.
Year 6 (6/30)	Set the mode, as transmitted	Set the timestamp to 12/31 of year 9, as transmitted	Not updated	On 6/30 of year 6, the retention controls are extended: ● The transmitted Object Lock Mode matches the version's currently stored mode. ● The transmitted Retain Until Date is set to 12/31 of year 9.
Year 9 (12/31)	Not updated	Not updated	Not updated	On 12/31 of year 9, retention controls expire; however, since its Legal Hold status is On, it is not eligible for deletion.
Year 10 (6/30)	Not updated	Not updated	Set to Off, as transmitted	On 6/30 of year 10, the Legal Hold status is set to Off, and thereafter, no Object Lock protections apply, and the version is eligible for deletion.

The bucket's default retention configurations may be overridden by transmitting any explicit Object Lock value with the object:

- To apply explicit Object Lock retention values, transmit all applicable Object Lock values (i.e., retention values and, if applicable, Legal Hold status) with the object when it is stored. See Section A.1.2, *Explicitly Transmitting Fixed Retention with the Object*, for additional information.
- Transmitting the Legal Hold status, set to On or Off, with the object when it is stored prevents bucket default retention controls from being applied. *Cohasset cautions that this results in storing objects without retention controls and, therefore, is not in compliance with the Rules.*

A.1.2 Explicitly Transmitting Fixed Retention with the Object

Explicit Object Lock retention values should be transmitted with an object when (a) bucket defaults are not configured, (b) bucket defaults do not satisfy the retention requirements of a specific object version or (c) the source system can reliably determine and transmit the appropriate Object Lock settings during object creation. The Legal Hold status may also be explicitly set when the object is stored.

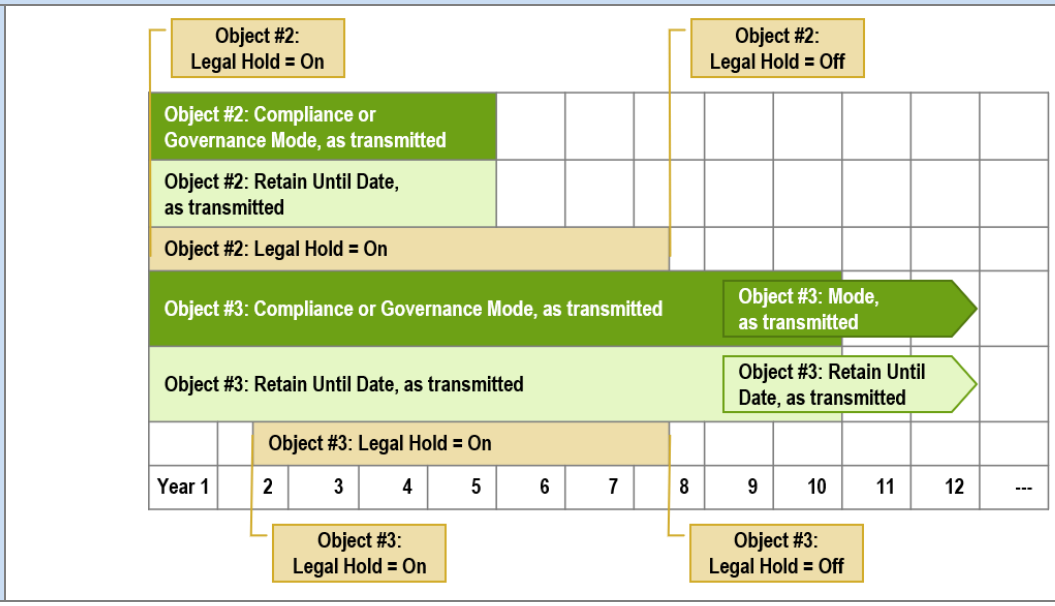
This approach requires Object Lock retention values to be transmitted with each object version stored in the bucket. Further, each transmitted Object Lock value must meet the applicable bucket and IAM policy conditions; see Appendix A.3, *Condition Keys for Bucket and IAM Policies*, for more information.

If retention values are not transmitted with the object and bucket defaults are not configured, Object Lock retention protections are not applied. Accordingly, regulated entities may prefer to configure bucket default retention controls to consistently apply retention controls to objects stored in the bucket. Then, transmit explicit Object Lock retention values when the bucket defaults are not appropriate. For additional information, see Section A.1.1, *Configuring and Relying on Bucket Defaults for Fixed Retention*.

A.1.2.1 Example B: Fixed retention (transmitted values applied), with retention extension and Legal Hold

Example B illustrates fixed retention and Legal Hold values applied as transmitted values for Object #2 and Object #3, which are specific object versions. The operations to manage each version's retention and Legal Hold values are described in the table below the illustration.

Example B: Fixed Retention (transmitted values applied), with retention extension and Legal Hold



Example B: Fixed Retention (transmitted values applied), with retention extension and Legal Hold				
	Object Lock Mode	**Retain Until Date**	**Legal Hold**	**Operations**
Object #2 creation	Set the mode, as transmitted	Set the timestamp to 12/31 of year 5, as transmitted	Set to On, as transmitted	At creation, **Object #2** is transmitted with explicit Object Lock values, which are stored as version metadata: ● The Object Lock Mode is set to the **transmitted** value. ● The Retain Until Date is set to the **transmitted** timestamp of 12/31 of year 5. ● The Legal Hold status is set to On, as transmitted Important Note: To apply both retention and Legal Hold values at object creation, the version must be transmitted with all applicable Object Lock values, including both retention values and Legal Hold status.
Object #3 creation	Set the mode, as transmitted	Set the timestamp to 12/31 of year 10, as transmitted	Not set	At creation, **Object #3** is transmitted with explicit Object Lock values, which are stored as version metadata: ● The Object Lock Mode is set to the **transmitted** value. ● The Retain Until Date is set to the **transmitted** timestamp of 12/31 of year 10.
Year 2 (6/30)	Not updated	Not updated	Set to On, as transmitted	On 6/30 of year 2, for **Object #3**, the transmitted Legal Hold status is set to On.
Year 5 (12/31)	Not updated	Not updated	Not updated	On 12/31 of year 5, for **Object #2**; retention controls expire, however, since its Legal Hold status is On, it is not eligible for deletion.
Year 8 (6/30)	Not updated	Not updated	Set to Off, as transmitted	On 6/30 of year 8, for **Object #2** and **Object #3**, the transmitted Legal Hold status is separately set to Off: ● **Object #2** is no longer protected by Object Lock controls and is eligible for deletion. ● **Object #3** remains protected by Object Lock retention controls and is not eligible for deletion.
Year 9 (3/15)	Set the mode, as transmitted	Set the timestamp to 12/31 of year 12, as transmitted	Not updated	On 3/15 year 9, for **Object #3**, retention controls are extended: ● The transmitted Object Lock Mode matches the version's currently stored mode. ● The transmitted Retain Until Date is set to 12/31 of year 12.
Year 12 (12/31)	Not updated	Not updated	Not updated	On 12/31 of year 12, for **Object #3**, retention controls expire, and it is eligible for deletion.

A.2 Guidance for Variable Retention Controls

By definition, variable retention periods require keeping records indefinitely until a specified business event occurs (e.g., termination or contract expiration), after which the record is kept for a post-event retention requirement, (e.g., 6 Years for a retention period of Termination + 6 Years). Business need or regulatory amendment may require future changes to the retention period. For example, a retention period of Termination + 6 Years may change to Termination + 10 Years.

With variable retention, the following retention values will be stored as version metadata to prevent deletion:

1. The **Object Lock Mode** of Compliance (highly restrictive) or Governance (less restrictive).
2. The **Event Hold** is set to On and the **Event Hold Duration** is set.
   - When the Event Hold is set to On, variable retention is active and the version is not eligible for deletion.
   - When the Event Hold is changed from On to Off, S3 adds the version's current Event Hold Duration to the Current Time and updates the Retain Until Date with the calculated value only if it is *greater* than the version's currently stored Retain Until Date; otherwise, the Retain Until Date is not updated.
   - The Event Hold Duration can be updated at any time when the Event Hold is set to On. When updated, S3 recalculates the Retain Until Date using the *greater* of the previous and updated Event Hold Duration values added to the Current Time. The recalculated value is stored only if it is *greater* than the version's currently stored Retain Until Date; otherwise, the Retain Until Date is not updated. Thus, changes to the Event Hold Duration will not reduce the version's Retain Until Date, though it may be extended.
3. The **Retain Until Date**, which may be system calculated (as described above) or explicitly transmitted with the version. Cohasset strongly recommends setting the Retain Until Date to the shortest retention requirement for the record (e.g., 6 Years for the retention period of Termination + 6 Years) during record creation or within 24 hours to prevent alteration, replacement, or deletion before the initial Retain Until Date expires.
   - When the Object Lock Mode is set to Compliance, S3 ensures that the version's Retain Until Date cannot be reduced by any user, and no user can prematurely delete the version.
   - When the Object Lock Mode is set to Governance, S3 ensures that only privileged users with *BypassGovernanceRetention* permission can reduce the Retain Until Date or prematurely delete the version.

Retention controls are applied to versions during record creation by either:

1. **Configuring and Relying on Bucket Defaults for Variable Retention** and not transmitting specific Object Lock retention or Legal Hold values with the object when bucket defaults are being applied, or
2. **Explicitly Transmitting Variable Retention with the Object** and not relying on bucket default retention values. Reminder: Transmitting explicit Object Lock values with the object overrides any bucket defaults.

Each approach is described in the following subsections, with examples illustrating how retention is applied and managed. In all examples, Cohasset assumes that *BypassGovernanceRetention* permissions are not used.

A.2.1 Configuring and Relying on Bucket Defaults for Variable Retention

Cohasset recommends configuring bucket defaults for Object Lock retention on all buckets that may store required records. These bucket defaults can be configured to apply controls for variable retention. When configured, bucket defaults help ensure retention controls are applied consistently when records are stored, without requiring source systems to transmit explicit retention values with each record.

When bucket default retention configurations do not meet the retention requirements for a particular record, the source system can transmit explicit Object Lock retention values with the object during storage, and these explicit values override the bucket defaults. For additional information, see Section A.2.2, *Explicitly Transmitting Variable Retention with the Object*.

Cohasset has identified different approaches to configuring bucket default retention:

1. **Least Restrictive Retention Controls:** Configure bucket defaults to meet the least restrictive variable retention requirements. For example, if the bucket will store records with retention periods of both Termination + 3 Years and Termination + 6 Years, configure the bucket defaults to apply the shorter 3-Year post-event retention requirement. Then, transmit explicit Object Lock retention values for records requiring more restrictive retention.
2. **Most Restrictive Retention Controls:** Configure bucket defaults to align with the most restrictive variable retention requirements (e.g., longest retention period). Then, transmit explicit Object Lock retention values for records requiring less restrictive retention protections.
3. **Most Common Retention Controls:** Configure bucket defaults to align with the most common variable retention requirements for records stored in the bucket. Then, transmit explicit Object Lock retention values only when different retention settings are needed.

The following table summarizes the bucket default configurations for variable retention The default values must satisfy the bucket and IAM policy conditions; see Appendix A.3, *Condition Keys for Bucket and IAM Policies*, for more information.

Default Parameter	Bucket default configurations for variable retention
Default Object Lock Mode	● Configure this default to either highly restrictive **Compliance** mode or less restrictive **Governance** mode. ○ If configuring to less restrictive Governance mode, plan and implement procedural controls to monitor reductions to the Retain Until Dates and removal of Object Lock retention controls.
Default Retention Period (optional) **and** **Default Event Hold Duration (required)**	● Either the **Default Retention Period** or the **Default Event Hold Duration** is used to calculate the version's initial Retain Until Date during object creation, unless Object Lock retention or Legal Hold values are explicitly transmitted with the version; therefore, these defaults should be planned together. ○ If the optional **Default Retention Period** is configured, it must be greater than or equal to the **Default Event Hold Duration**, and S3 adds it to the version's creation/storage timestamp to calculate the initial Retain Until Date. ○ Otherwise, S3 adds the **Default Event Hold Duration** to the version's creation/storage timestamp to calculate the initial Retain Until Date. ● Additionally, when the version's **Event Hold** transitions from On to Off, S3 adds the version's **Event Hold Duration** to the Current Time to calculate the post-event **Retain Until Date**, which is stored only if it is greater than the version's currently stored **Retain Until Date**.

Default Parameter	Bucket default configurations for variable retention
	Default Retention Period (optional) ● S3 supports a bucket **Default Retention Period** range of 1 day to 100 years. ● Cohasset strongly recommends always configuring the **Default Retention Period** to satisfy[27] the post-event retention requirement (e.g., 6 Years for a retention period of Termination + 6 Years). This ensures that the version's initial Retain Until Date is set to the shortest time that the record must be kept and applies strong controls to prevent alteration, replacement, or deletion. ○ When Object Lock is applied in Compliance mode, a version's Retain Until Date cannot be reduced after it is applied. **Default Event Hold Duration (required)** ● S3 supports a **Default Event Hold Duration** range of 1 day to 100 years. ● Cohasset recommends configuring the **Default Event Hold Duration** as follows: ○ Configure it to match the post-event retention requirement, when the Event Hold will transition from On to Off soon after the business event occurs. ○ Configure it for a shorter period when the Event Hold will transition from On to Off long after the business event occurs, provided the source system will transmit each version's updated Retain Until Date when its Event Hold is transitioned to Off. ● See **Example C** where both the bucket **Default Retention Period** and **Default Event Hold Duration** are configured to the post-event retention requirement. ● See **Example D** where only the bucket **Default Retention Period** is configured to the post-event retention requirement and the bucket **Event Hold Duration** is considerably shorter and the source system transmits an updated Retain Until Date when the Event Hold transitions to Off. ● See **Example E**, which Cohasset asserts is **not** compliant with the Rules, because the planned retention period is Termination + 6 Years but the bucket defaults set the initial Retain Until Date to only 183 Days (6 Months) when the version is stored. Cohasset asserts that this is out of compliance when the required retention period is Termination + 6 Years, because the shortest retention obligation for the record is 6 Years.

Cohasset recommends setting legal holds only after the object is stored, as needed, to suspend deletion eligibility until the Legal Hold is cleared (Off). When Legal Hold is cleared, Object Lock retention protections continue to govern deletion eligibility. Important Note: If a Legal Hold status (On or Off) is transmitted with the object during creation, the bucket defaults for Object Lock retention will not be applied to the object. Since Legal Holds are a simple On/Off, Cohasset did not insert operations for setting and clearing Legal Holds for the following examples.

A.2.1.1 Example C: Variable retention (bucket defaults applied), Default Retention Period and Event Hold Duration are configured to the post-event retention requirement

Example C illustrates retention controls for a variable retention period of Termination + 6 Years, when the following bucket defaults are configured as follows:

- **Bucket Default Object Lock Mode** is configured to Compliance or Governance.
- **Bucket Default Event Hold Duration** is configured to 2,190 Days (or 6 Years).
- **Bucket Default Retention Period** is configured to 6 Years.

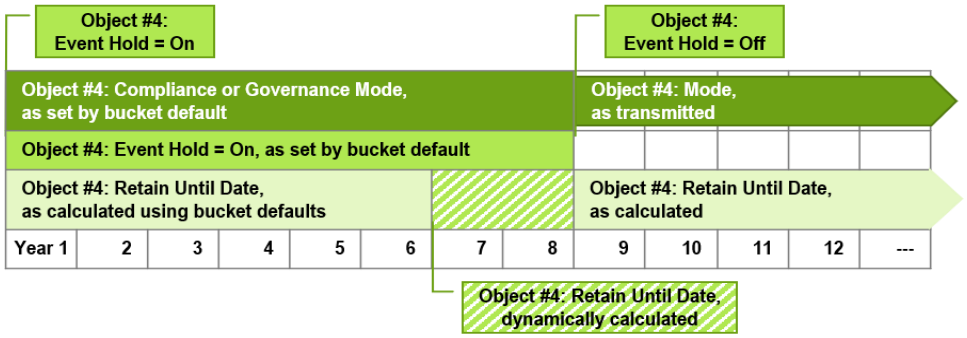
[27] If the regulated entity's internal retention standard is longer than the regulatory requirement, Cohasset recommends collaborating with the Compliance Officer and business operations to determine whether the Default Retention Period should be configured with the regulatory requirement or the entity's longer internal retention standard.

For this example, both the bucket **Default Retention Period** and **Default Event Hold Duration** are configured to the post-event retention requirement.

- This ensures that the version's initial Retain Until Date is set to the shortest time that the record must be kept and applies strong controls to prevent alteration, replacement, or deletion.
- Also, S3 automatically applies the post-event retention requirement to the version when its Event Hold transitions from On to Off, provided no user changed the version's Event Hold Duration.

These bucket defaults are used to store metadata for Object #4, which is a specific object version. The operations to manage the version's retention values are described in the table below the illustration.

Example C: Variable retention (bucket defaults applied), Default Retention Period and Event Hold Duration are configured to the post-event retention requirement



	Object Lock Mode	Event Hold	Event Hold Duration	Retain Until Date	Operations
Object #4 creation	Set the mode to the bucket default value	Set to On to activate variable retention, when the bucket default Event Hold Duration is applied	Set to 2,190 Days (i.e., 6 Years), per bucket default	Set the timestamp, as **calculated** using bucket defaults	At creation, Object #4 is stored without transmitting explicit retention values or a Legal Hold status: • The Object Lock Mode is stored by applying the bucket Default Object Lock Mode. • The Event Hold is set to On, when the bucket Default Event Hold Duration is applied. • The Event Hold Duration is set to 2,190 Days, which is the bucket Default Event Hold Duration. • The Retain Until Date is stored as 12/31 of year 6, by adding the bucket **Default Retention Period** (i.e., 6 Years) to the version's creation/storage timestamp. • The version's Legal Hold status must not be set when applying bucket retention defaults.
Year 6 (12/31)	Not updated	Not updated	Not updated	Dynamically calculated (not stored)	On 12/31 of year 6, for Object #4, the stored Retain Until Date expires; however, the Event Hold remains set to On, which provides continued Object Lock retention protection and dynamically calculates and displays the Retain Until Date of Event Hold Duration + Current Time.

Example C: Variable retention (bucket defaults applied), Default Retention Period and Event Hold Duration are configured to the post-event retention requirement					
Year 8 (12/31)	Set the mode, as transmitted	Set to Off, as transmitted to transition from variable to fixed retention	Update is prohibited	Set the timestamp, as **calculated** using the version's Event Hold Duration	On 12/31 of year 8, for Object #4, when the business event occurs, the version's retention values are updated: • The transmitted Object Lock Mode matches the version's currently stored mode. • The transmitted Event Hold value is set to Off, which transitions the version from variable to fixed retention. • Note: The Event Hold Duration cannot be transmitted when setting Event Hold to Off. • An explicit Retain Until Date is optional but is not transmitted for this operation. Therefore, S3 automatically calculates the post-event Retain Until Date by adding the version's **Event Hold Duration** (2.190 Days) + Current Time, and since it is greater than the version's currently stored Retain Until Date, the calculated Retain Until Date is stored.
Year 14 (12/31)	Not updated	Not updated	Not updated	Not updated	On approximately 12/31 of year 14, for Object #4, retention controls expire, and it is eligible for deletion.

A.2.1.2 Example D: Variable retention (bucket defaults applied), Default Retention Period is configured to the post-event retention requirement, Event Hold Duration is configured to a short duration

Example D illustrates retention controls for a variable retention period of Termination + 6 Years, when the following bucket defaults are configured as follows. To facilitate comparison with Example C, the bucket default configurations that differ from those in Example C are highlighted in **blue font**.

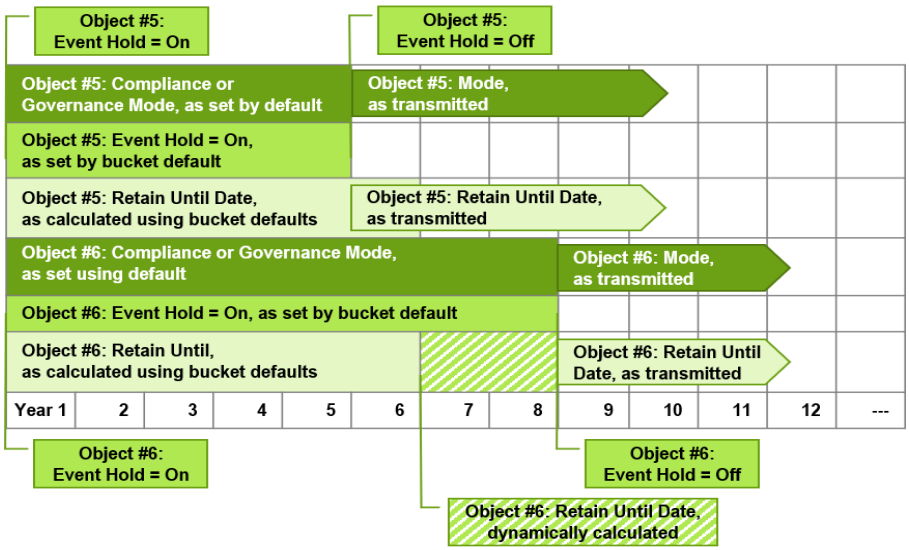
- **Bucket Default Object Lock Mode** is configured to Compliance or Governance.
- **Bucket Default Event Hold Duration** is configured to **183 Days (6 Months)**.
- **Bucket Default Retention Period** is configured to 6 Years.

For this example, only the bucket **Default Retention Period** is configured to the post-event retention requirement, and the bucket Event Hold Duration is considerably shorter.

- The bucket **Default Retention Period** ensures that the version's initial Retain Until Date is set to the shortest time that the record must be kept (e.g., 6 Years) and applies strong controls to prevent alteration, replacement, or deletion.
- To ensure the record's full retention requirement is met when the version's Event Hold transitions from On to Off, the source system should calculate and transmit the Retain Until Date, because the version's Event Hold Duration of 183 Days is unlikely to meet the record's full retention obligation.

These bucket defaults are used to store metadata for Object #5 and Object #6, which are specific object versions. The operations to manage the version's retention values are described in the table below the illustration.

Example D: Variable retention (bucket defaults applied), Default Retention Period is configured to the post-event retention requirement, Event Hold Duration is configured to a short duration



	Object Lock Mode	Event Hold	Event Hold Duration	Retain Until Date	Operations
Object #5 creation and Object #6 creation	Set the mode to the bucket default value	Set to On to activate variable retention, when the bucket default Event Hold Duration is applied	Set to **183 Days** (i.e., 6 Months), per bucket default	Set the timestamp, as **calculated** using bucket defaults	At creation, **Object #5** and **Object #6** are stored without transmitting explicit retention values or a Legal Hold status; thus, these two objects have the same initial retention settings: • The Object Lock Mode is stored by applying the bucket Default Object Lock Mode. • The Event Hold is set to On, when the bucket Default Event Hold Duration is applied. • The Event Hold Duration is set to **183 Days**, which is the bucket Default Event Hold Duration. • The Retain Until Date is set to 12/31 of year 6, by adding the bucket **Default Retention Period** to the object's creation/storage timestamp. • The version's Legal Hold status must not be set when applying bucket retention defaults.
Year 5 (12/31)	Set the mode, as transmitted	Set to Off, as transmitted to transition from variable to fixed retention	Update is prohibited	Set the timestamp to 6/30 of year 10, as transmitted	On 12/31 of year 5, for **Object #5**, when the business event occurs, the version's retention values are updated: • The transmitted Object Lock Mode matches the version's currently stored mode. • The transmitted Event Hold value is set to Off, which transitions the version from variable to fixed retention. • Note: The Event Hold Duration cannot be transmitted when setting Event Hold to Off. • An explicit Retain Until Date is optional and is transmitted as 6/30 of year 10, which is the final retention period for the record.

Example D: Variable retention (bucket defaults applied), Default Retention Period is configured to the post-event retention requirement, Event Hold Duration is configured to a short duration					
					• Note: If an explicit Retain Until Date were not transmitted, S3 would calculate a new Retain Until Date by adding the version's **Event Hold Duration** (183 Days) + Current Time, and since it is *less* than the version's currently stored Retain Until Date, it is not updated. Given the retention period of Termination + 6 Years, it is unlikely that the initial Retain Until Date accurately represents the full retention period. Therefore, the source system needs to transmit the Retain Until Date, as was done in this row.
Year 6 (12/31)	Not updated	Not updated	Not updated	Dynamically calculated (not stored)	On 12/31 of year 6, for **Object #6**, the stored Retain Until Date expires; however, the Event Hold remains set to On, which provides Object Lock retention protections and dynamically calculates and displays the Retain Until Date of Event Hold Duration + Current Time.
Year 8 (12/31)	Set the mode, as transmitted	Set to Off, as transmitted to transition from variable to fixed retention	Update is prohibited	Set the timestamp to 3/31 of year 12, as transmitted	On 12/31 of year 8, for **Object #6**, when the business event occurs, the version's retention values are updated: • The transmitted Object Lock Mode matches the version's currently stored mode. • The transmitted Event Hold value is set to Off, which transitions the version from variable to fixed retention. • Note: The Event Hold Duration cannot be transmitted when setting Event Hold to Off. • An explicit Retain Until Date is optional and is transmitted as 3/31 of year 12, which is the final retention period for the record. • Note: If an explicit Retain Until Date were not transmitted, S3 would calculate a new Retain Until Date by adding the version's **Event Hold Duration** (183 Days) + Current Time, and since it is *greater* than the version's currently stored Retain Until Date, the calculated Retain Until Date would be stored. Given the retention period of Termination + 6 Years, it is unlikely that the calculated Retain Until Date accurately represents the full retention period. Therefore, the source system needs to transmit the Retain Until Date, as was done in this row.
Year 10 (6/30)	Not updated	Not updated	Not updated	Not updated	On 6/30 of year 10, for **Object #5**, retention controls expire, and it is eligible for deletion.
Year 12 (3/31)	Not updated	Not updated	Not updated	Not updated	On 3/31 of year 12, for **Object #6**, retention controls expire, and it is eligible for deletion.

A.2.1.3 Example E: Variable retention (bucket defaults applied), Default Retention Period is not configured and Event Hold Duration is configured to a short duration; Cohasset asserts this is not compliant with SEC Rules

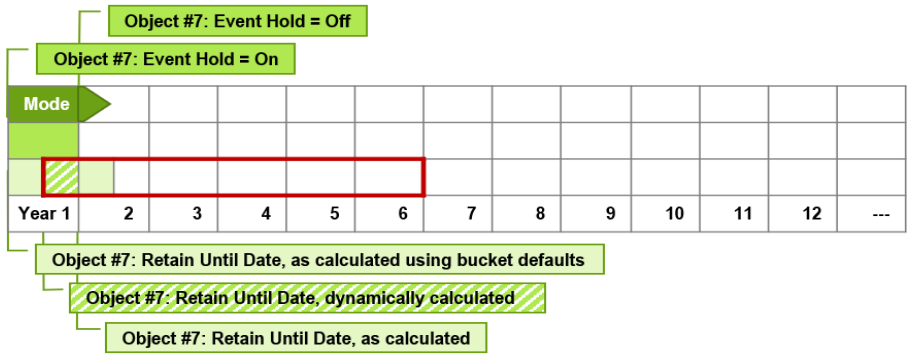
Example E illustrates retention controls for a variable retention period of Termination + 6 Years, when the following bucket defaults are configured as follows. Cohasset asserts that Example E is **not** compliant with the requirements of the Rules, even though the bucket configurations are similar to Example D. To facilitate comparison with Example D, the bucket default configurations that differ from those in Example D are highlighted in **red font**.

- **Bucket Default Object Lock Mode** is configured to Compliance or Governance.
- **Bucket Default Event Hold Duration** is configured to **183 Days** (6 Months).
- **Bucket Default Retention Period** is **not configured**.

Important Note: Cohasset asserts that Default Event Hold Duration or Default Retention Period must be configured to the shortest retention obligation for the record (e.g., 6 Years) to apply strong retention controls when the record is stored to prevent alteration, replacement, and deletion for compliance with the Rules. This example does not accomplish this and therefore should not be considered a compliant configuration.

These bucket defaults are used to store metadata for Object #7, which is a specific object version. The operations to manage the version's retention values are described in the table below the illustration.

Example E: Variable retention (bucket defaults applied), Default Retention Period is not configured, and Event Hold Duration is configured to a short duration; Cohasset asserts this is not compliant with SEC Rules



	Object Lock Mode	Event Hold	Event Hold Duration	Retain Until Date	Operations
Object #7 creation	Set the mode to the bucket default value	Set to On to activate variable retention, when the bucket default Event Hold Duration is applied	Set to **183 Days** (i.e., 6 Months), per bucket default	Set the timestamp, as **calculated** using bucket defaults	At creation, Object #7 is stored without transmitting explicit retention values or a Legal Hold status: • The Object Lock Mode is stored by applying the bucket Default Object Lock Mode. • The Event Hold is set to On, when the bucket Default Event Hold Duration is applied. • The Event Hold Duration is set to **183 Days**, which is the bucket Default Event Hold Duration. • The Retain Until Date is set by adding the bucket **Default Event Hold Duration** (**183 Days**) to the object's creation/storage timestamp. Note: Cohasset asserts this **does not comply with the Rules**, because the initial Retain Until

Example E: Variable retention (bucket defaults applied), Default Retention Period is not configured, and Event Hold Duration is configured to a short duration; Cohasset asserts this is not compliant with SEC Rules					
					Date must be set to the shortest retention obligation for the record (e.g., 6 Years) to apply strong retention controls when the record is stored to prevent alteration, replacement, and deletion for compliance with the Rules. Therefore, this is out of compliance because the Retain Until Date is set to only **183 Days**, by adding the bucket **Default Event Hold Duration** to the object's creation/storage timestamp. This gap in retention protections is outlined in red. ● The version's Legal Hold status must not be set when applying bucket retention defaults.
Year 1 (6/30)	Not updated	Not updated	Not updated	Dynamically calculated (not stored)	**After 183 Days** (6 Months), for Object #7, the stored Retain Until Date expires; however, the Event Hold remains set to On, which provides Object Lock retention protections and dynamically calculates and displays the Retain Until Date of Event Hold Duration + Current Time.
Year 1 (12/31)	Set the mode, as transmitted	Set to Off, as transmitted to transition from variable to fixed retention	Update is prohibited	Set the timestamp, as **calculated** using the version's Event Hold Duration	On 12/31 of year 1, for **Object #7**, when the business event occurs, the version's retention values are updated: ● The transmitted Object Lock Mode matches the version's currently stored mode. ● The transmitted Event Hold value is set to Off, which transitions the version from variable to fixed retention. ● Note: The Event Hold Duration cannot be transmitted when setting Event Hold to Off ● An explicit Retain Until Date is optional but is not transmitted in this operation. Therefore, S3 automatically calculates the post-event Retain Until Date by adding the version's **Event Hold Duration** (183 Days) + Current Time, and since it is greater than the version's currently stored Retain Until Date, the calculated Retain Until Date is stored. Note: Transmitting an explicit Retain Until Date would not resolve the compliance gap described in the row related to object creation.
Year 12 (3/31)	Not updated	Not updated	Not updated	Not updated	On 3/31 of year 12, for Object #7, retention controls expire, and it is eligible for deletion.

The bucket's default retention settings may be overridden by transmitting explicit Object Lock values with the object:

- To apply explicit retention values, transmit the Object Lock retention values with the object when it is stored. See Section A.2.2, *Explicitly Transmitting Variable Retention with the Object*, for additional information.
- To apply both retention values and Legal Hold status, transmit the Object Lock values with the object when it is stored.
- Transmitting the Legal Hold status, set to On or Off, with the object when it is stored prevents bucket default retention controls from being applied. *Cohasset cautions that this results in storing objects without retention controls and, therefore, not in compliance with the Rules*.

A.2.2 Explicitly Transmitting Variable Retention with the Object

Explicit Object Lock retention values should be transmitted with an object when (a) bucket defaults are not configured, (b) bucket defaults do not satisfy the retention requirements of a specific object version or (c) the source system can reliably determine and transmit the appropriate Object Lock settings during object creation. The Legal Hold status may also be explicitly set when the object is stored.

In this example, Object Lock retention values are transmitted with each object version stored in the bucket. For compliance with the Rules, Cohasset asserts that the Retain Until Date transmitted with the object version must meet the full post-event retention requirement (e.g., 6 Years for a retention period of Termination + 6 Years). Further, each Object Lock value must meet the bucket and IAM Policy conditions; see Appendix A.3, *Condition Keys for Bucket and IAM Policies*, for more information.

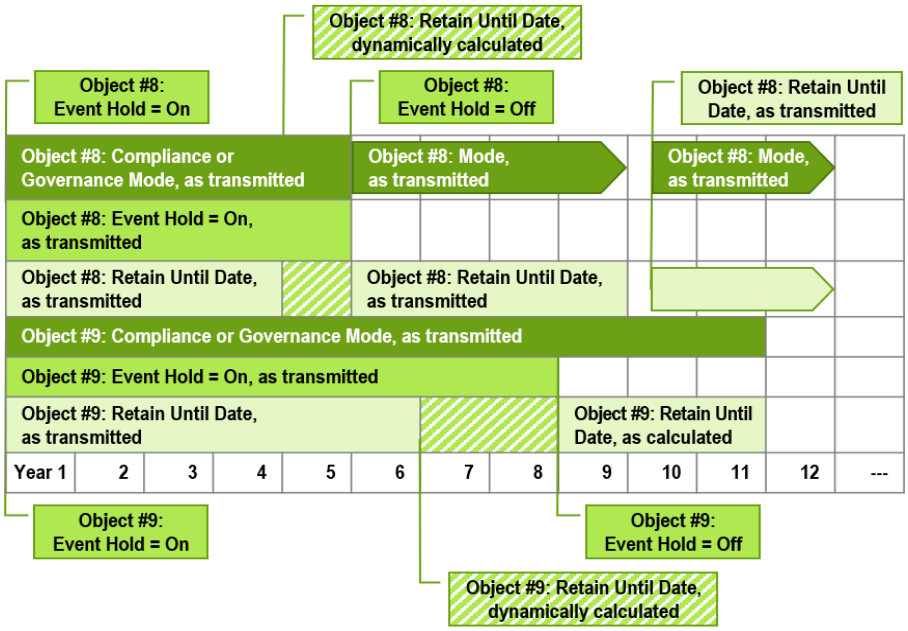
If retention values are not transmitted with the object and bucket defaults are not configured, Object Lock retention protections are not applied to the version when it is stored. Accordingly, regulated entities may prefer to establish bucket default retention settings to consistently apply retention controls to objects stored in the bucket. Then, transmit explicit Object Lock retention values when the bucket defaults are not appropriate. For additional information, see Section A.2.1, *Configuring and Relying on Bucket Defaults for Variable Retention*.

A.2.2.1 Example F: Variable Retention (transmitted values applied), with retention extension

Example F illustrates variable retention protections applied as transmitted values for Object #8 and Object #9, which are specific object versions. Though the Legal Hold feature is not depicted in the following, it may be set and cleared on an object version at any time and is independent of the Object Lock retention controls.

The operations to manage each version's retention values are described in the table below the illustration.

Example F: Variable Retention (transmitted values applied), with retention extension



	Object Lock Mode	Event Hold	Event Hold Duration	Retain Until Date	Operations
Object #8 creation	Set the mode, as transmitted	Set to On, as transmitted to apply variable retention	Set to 1,095 days (3 years), as transmitted	Set the timestamp to 12/31 of year 4, as transmitted	At creation, **Object #8** is transmitted with explicit Object Lock values, which are stored as version metadata: • The Object Lock Mode is set to the transmitted value. • The Event Hold is set to the **transmitted** value of On for variable retention. • The Event Hold Duration is set to the **transmitted** value of 1,095 Days (3 Years). • The Retain Until Date is set to the **transmitted** timestamp of 12/31 of year 4 Note: Transmitting the Retain Until Date is optional, if it were not transmitted, the calculated value of 12/31 of year 3 (**Event Hold Duration** + Current Time) would be stored.
Object #9 creation	Set the mode, as transmitted	Set to On, as transmitted to apply variable retention	Set to 1,095 days (3 years), as transmitted	Set the timestamp to 12/31 of year 6, as transmitted	At creation, **Object #9** is transmitted with explicit Object Lock values, which are stored as version metadata: • The Object Lock Mode is set to the transmitted value. • The Event Hold is set to the **transmitted** value of On for variable retention. • The Event Hold Duration is set to the **transmitted** value of 1,095 Days (3 Years). • The Retain Until Date is set to the **transmitted** timestamp of 12/31 of year 6.

Example F: Variable Retention (transmitted values applied), with retention extension					
Year 4 (12/31)	Not updated	Not updated	Not updated	Dynamically calculated (not stored)	On 12/31 of year 4, for **Object #8**, the stored Retain Until Date expires; however, the Event Hold remains set to On, which provides Object Lock retention protections and dynamically calculates and displays the Retain Until Date of Event Hold Duration + Current Time.
Year 5 (12/31)	Set the mode, as transmitted	Set to Off, as transmitted to transition from variable to fixed retention	Update is prohibited	Set the timestamp to 12/31 of year 9, as transmitted	On 12/31 of year 5, for **Object #8**, when the business event occurs, the retention values are updated: ● The transmitted Object Lock Mode matches the version's currently stored mode. ● The transmitted Event Hold value is set to Off, which transitions the version from variable to fixed retention. ● The transmitted post-event Retain Until Date is set to 12/31 of year 9.
Year 6 (12/31)	Not updated	Not updated	Not updated	Dynamically calculated (not stored)	On 12/31 of year 6, for **Object #9**, the stored Retain Until Date expires; however, the Event Hold remains set to On, which provides Object Lock retention protections and dynamically calculates and displays the Retain Until Date of Event Hold Duration + Current Time.
Year 8 (12/31)	Set the mode, as transmitted	Set to Off, as transmitted to transition from variable to fixed retention	Update is prohibited	Set the timestamp, as **calculated** using the version's Event Hold Duration	On 12/31 of year 8, for **Object #9**, when the business event occurs, the retention values are updated: ● The transmitted Object Lock Mode matches the version's currently stored mode. ● The transmitted Event Hold value is set to Off, which transitions the version from variable to fixed retention. ● An explicit Retain Until Date is optional but is not transmitted, in this operation; therefore, S3 automatically updates the post-event Retain Until Date by adding the version's **Event Hold Duration** (1,095 Days) + Current Time, and since it is greater than the version's currently stored Retain Until Date, the calculated Retain Until Date is stored.
Year 10 (3/31)	Set the mode, as transmitted	Not updated	Not updated	Set the timestamp to 12/31 of year 12, as transmitted	On 3/31 of year 10 for **Object #8**, fixed retention controls are applied to the version (assuming the object version was not deleted when it was not protected by retention), using transmitted values: ● The transmitted Object Lock Mode matches the version's currently stored mode. ● The transmitted Retain Until Date is set to 12/31 of year 12.

Example F: Variable Retention (transmitted values applied), with retention extension					
Year 11 (12/31)	Not updated	Not updated	Not updated	Not updated	On 12/31 of year 11, for **Object #9**, retention controls expire, and it is eligible for deletion.
Year 12 (12/31)	Not updated	Not updated	Not updated	Not updated	On 12/31 of year 12, for **Object #8**, retention controls expire, and it is eligible for deletion.

A.3 Condition Keys for Bucket and IAM Policies

Bucket and IAM policies can be used to control access to Amazon S3 resources and define allowed and denied operations. These policies may also include condition keys, which provide additional guardrails for object-level operations.

- Bucket policies are resource-based policies that apply to a bucket and the objects stored in it. Each operation is evaluated against the bucket policy, including any configured condition keys, to determine whether the operation is allowed or denied. As a result, bucket policies apply consistent restrictions to all users and applications accessing the bucket.
- IAM policies are identity-based policies that apply to operations issued by users, groups, and roles. Each operation is evaluated against the applicable IAM policy, including any configured condition keys, to determine whether the operation is allowed or denied. As a result, IAM policies enforce restrictions on specific users, groups, roles, and source systems, regardless of the bucket being accessed.

Amazon S3 supports several Object Lock-related condition keys that can be configured in bucket and IAM policies to validate Object Lock values. When Object Lock retention or Legal Hold values are stored with an object or are updated, the values must satisfy all applicable bucket and IAM policy requirements, including any configured condition keys. By using condition keys, regulated entities can enforce approved Object Lock settings, establish retention guardrails, and ensure that retention and Legal Hold controls align with organizational and regulatory requirements, whether applied through bucket defaults or explicitly transmitted.

The following table describes the condition keys relevant to Object Lock.

Condition key	**Description**
s3:object-lock-mode	• Evaluates the Object Lock Mode (i.e., Compliance or Governance) specified when storing Object Lock metadata. • It can be used to ensure that object versions are stored using only the approved Object Lock Mode and to prevent users or source systems from setting a mode that is not permitted.
s3:object-lock-retain-until-date	• Evaluates the Retain Until Date expressed as a timestamp (e.g., 2055-11-23T12:00:00Z) when storing Object Lock metadata. • It can be used to enforce minimum and maximum allowable timestamp for the Retain Until Date (i.e., allow or deny Retain Until Dates that are less than or greater than the setting). Accordingly, it can set a Min/Max range specified as a timestamp.

Condition key	Description
s3:object-lock-remaining-retention-days	• Evaluates the Retain Until Date expressed as remaining retention days (e.g., 2190 days) when storing Object Lock metadata. • It can be used to enforce minimum and maximum allowable Retain Until Date (i.e., allow or deny Retain Until Dates that are less than or greater than the setting). Accordingly, it can set a Min/Max range specified as days.
s3:object-lock-event-hold-duration-days	• Evaluates the Event Hold Duration expressed as days (e.g., 2190 days) when storing Object Lock metadata. • It can be used to enforce the minimum and maximum allowable Event Hold Durations.
s3:object-lock-event-hold	• Evaluates the Event Hold (i.e., On or Off) status specified when storing Object Lock metadata. • It can be used to mandate that Event Hold be set to On, to ensure that variable retention is applied, or it can require Event Hold be set to Off. Stated another way, it can be used to restrict whether Event Holds may be applied (On) or cleared (Off) and to ensure that Event Hold settings comply with organizational or regulatory requirements.
s3:object-lock-legal-hold	• Evaluates the Legal Hold (i.e., On or Off) status specified when storing Object Lock metadata. • It can be used to mandate that Legal be set to On, or require it be set to Off. Stated another way, it can be used to restrict whether Legal Holds may be applied or cleared and ensure that applied Legal Holds comply with organizational or regulatory requirements.

Appendix B • 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.

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

In 17 CFR § 240.17a-4 (SEC Rule 17a-4) for the securities broker-dealer industry and 17 CFR § 240.18a-6 (SEC Rule 18a-6) for nonbank SBS entities, the U.S. Securities and Exchange Commission (SEC) stipulates recordkeeping requirements, including retention periods.

In 2022, the SEC adopted amendments to SEC Rules 17a-4 and 18a-6, which define technology-neutral requirements for electronic recordkeeping systems. These 2022 amendments became effective on January 3, 2023, with compliance dates of May 3, 2023, for 17 CFR § 240.17a-4, and November 3, 2023, for 17 CFR § 240.18a-6.

> *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.*[28] [emphasis added]

These amendments allow regulated entities to use electronic recordkeeping systems that either (a) retain the records together with complete time-stamped audit trails or (b) retain records in a non-rewriteable, non-erasable (i.e., WORM or write-once, read-many) format.

> *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.*[29] [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. Also 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.

[28] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66428.

[29] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66419.

B.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 audit trails in business-purpose electronic recordkeeping systems.

> *[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.*[30] [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 enabling access to reproduction of the original record, 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.*[31] [emphasis added]

Further, the audit-trail requirement 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."*[32] [emphasis added]

B.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 of SEC Rules 17a-4(f) and 18a-6(e) continue to 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* *** [33] [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).

30 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.
31 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.
32 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66418.
33 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66419.

- *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).

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.*[34] [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.*[35] [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 software or hardware controls, or both, which protect preserved records 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.*[36] [emphasis added]

B.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).[37]

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.*

---

34 2003 Interpretative Release, 68 FR 25282.

35 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).

36 2003 Interpretative Release, 68 FR 25283.

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

B.3 Overview of CFTC Rule 1.31(c)-(d) *Electronic Regulatory Records* Requirements

In 17 CFR § 1.31 (CFTC Rule 1.31), the Commodity Futures Trading Commission (CFTC) stipulates recordkeeping requirements, including retention periods.

In 2017, the CFTC adopted amendments to CFTC Rule 1.31 to modernize and make technology-neutral the form and manner in which regulatory records must be kept. This resulted in less-prescriptive, principles-based requirements, which became effective on August 28, 2017.

> *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.*[38] [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 include both fixed and variable 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)*.

[38] 2017 CFTC Recordkeeping Requirements Adopting Release, 82 FR 24482.

Appendix C • Cloud Provider Undertaking

C.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.[39] [emphasis added]

C.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 both parties to take actions:
  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.

C.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) ensuring that the regulator has (when needed) access privileges, encryption keys, and other information and services to permit records to be accessed, downloaded, and transferred.

[39] 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.