Cohasset Associates

Amazon® Elastic Block Store (EBS)

COMPLIANCE ASSESSMENT

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

Abstract

Amazon® Web Services (AWS) is a secure cloud services platform hosted by Amazon to provide modular cloud-based products and services. Amazon Elastic Block Store (EBS) is an easy-to-use, scalable, high-performance block-storage service designed for Amazon Elastic Compute Cloud (EC2). The *Snapshot Lock* feature of Amazon EBS Snapshots is designed to meet securities industry requirements for preserving records in non-rewriteable, non-erasable format for the applied retention period and legal holds.

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

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

It is Cohasset's opinion that Amazon EBS Snapshots, when properly configured and used with *Snapshot Lock*, 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 EBS, with *Snapshot Lock*, 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.

November 2023

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

+1.312.527.1550 | www.cohasset.com

Table of Contents

1 • Introduction

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

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

1.1 Overview of the Regulatory Requirements

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

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

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

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

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

1.1.2 FINRA Rule 4511(c) Requirements

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

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

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

---

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

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

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

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

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

For additional information, refer to Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*, and Appendix A.3, *Overview of CFTC Rule 1.31(c)-(d) Electronic Regulatory Records Requirements*.

1.2 Purpose and Approach

To obtain an independent and objective assessment of the compliance capabilities of Amazon EBS Snapshots 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 EBS Snapshots, 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 EBS Snapshots; 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 EBS and its functionality or other Amazon products or services. The information utilized by Cohasset to conduct this assessment consisted of: (a) oral discussions, (b) product demonstrations, including system setup and configuration, (c) system documentation, (d) user and system administrator guides, and (e) 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 EBS Overview and Assessment Scope

1.3.1 Amazon EBS Overview

Amazon Web Services (AWS) is a secure cloud services platform hosted by Amazon to provide modular cloud-based products and services.

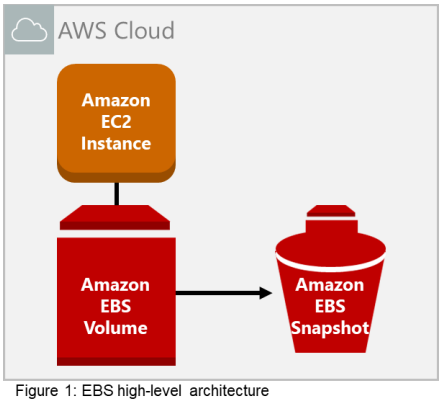

Figure 1: EBS high-level architecture

Amazon Elastic Compute Cloud (**EC2**) allows users to run virtual machines, referred to as Amazon EC2 **Instances**, on-demand. EC2 provides scalable compute capacity and an application programming interface (**EC2 API**) to enable programmatic service interactions.

Amazon Elastic Block Store (**EBS**) is a block storage service designed to be used with Amazon EC2 Instances. It stores data in **Volumes**, providing persistent, scalable, high-performance storage that can be attached to EC2 Instances.

Each EBS **Snapshot** is a point-in-time archival copy (replica) of a source EBS Volume and provides a recovery point to reestablish the archived records[4]. The Snapshot source may be (a) a single EBS Volume or (b) an entire Amazon EC2 Instance, which captures a separate Snapshot of each EBS Volume attached to the Instance. Snapshots are created asynchronously and are in a *pending* state until the Snapshot is *completed* (i.e., until all modified blocks have been transferred to Amazon S3).

The ***Snapshot Lock*** applies retention controls to disallow deletion for the specified lock duration, adding another layer of protection against inadvertent or malicious deletions of EBS Snapshots. The *Snapshot Lock* retention controls are designed to meet the SEC requirements for a non-rewriteable, non-erasable record format. *Snapshot Lock* may be set to *Compliance* or *Governance* mode.

- *Compliance* mode applies highly-restrictive controls, which disallow any user from (a) reducing or removing the lock duration, (b) downgrading the *Snapshot Lock* to Governance or (c) unlocking the *Snapshot Lock* retention controls, after the cooling-off period has expired.
- *Governance* mode applies less-restrictive controls, which allow users with special permissions to (a) reduce the lock duration, (b) upgrade *Snapshot Lock* to Compliance, or (c) unlock the *Snapshot Lock* retention controls.

1.3.2 Assessment Scope

The scope of this assessment is focused specifically on Snapshots of Amazon EBS Volumes when ***Snapshot Lock*** retention controls are applied in either *Compliance* (highly-restrictive) or *Governance* (less-restrictive) mode and an appropriate lock duration (*Lock Expiry Timestamp*) is applied to the Snapshot.

NOTE: At the time of this report:

- **Snapshot Lock** cannot be applied to Amazon Machine Images and cannot be applied using Data Lifecycle Manager (DLM) policies or other solutions.
- Also, this assessment excludes AWS infrastructure running on-premises with AWS Outposts.

[4] The SEC uses the phrase *books and records* to describe information that must be retained for regulatory compliance. In this report, Cohasset typically uses the term *record* or *Snapshot* (versus data, object or file) to recognize that the content may be required for regulatory compliance.

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 EBS Snapshots, for compliance with the electronic recordkeeping system requirements promulgated in SEC Rules 17a-4(f)(2) and 18a-6(e)(2), as well as describes how the solution supports the regulated entity in meeting the audit system requirement of SEC Rules 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii).

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

- ***Compliance Requirement*** – Excerpt of relevant regulatory requirement in SEC Rules 17a-4(f) and 18a-6(e) and Cohasset's interpretation of the specific requirement
  - Both SEC Rules 17a-4(f) and 18a-6(e) are addressed in this section, since the electronic recordkeeping system requirements (principles, controls and testable outcomes) are the same, though the Rules specify their respective regulations and regulators and include semantic differences.
- ***Compliance Assessment*** – Summary statement assessing compliance of Amazon EBS Snapshots
- ***Amazon EBS Snapshot 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 EBS Snapshots, as described in Section 1.3, *Amazon EBS Overview and Assessment Scope*, relative to the enumerated requirements of SEC Rules 17a-4(f) and 18a-6(e).

2.1 Record and Audit-Trail

2.1.1 Compliance Requirement

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

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

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

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

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

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

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

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

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

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

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

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

2.1.2 Compliance Assessment

In this report, Cohasset has not assessed EBS Snapshots or *Snapshot Lock* in comparison to this requirement of the SEC Rules.

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

Reminder: This requirement is an alternative to the non-rewriteable, non-erasable record format requirement (i.e., write-once, read-many or WORM requirement), which is assessed in Section 2.2.

2.2 Non-Rewriteable, Non-Erasable Record Format

2.2.1 Compliance Requirement

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

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

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

> *The 2003 interpretation clarified that the WORM requirement does not mandate the use of optical disks and, therefore, a broker-dealer can use "an electronic storage system that prevents the overwriting, erasing or otherwise altering of a record during its required retention period through the use of integrated hardware and software [control] codes." The*

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

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

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

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

> *[A] broker-dealer must take appropriate steps to ensure that records are not deleted during periods when the regulatory retention period has lapsed but other legal requirements mandate that the records continue to be maintained, and the broker-dealer's storage system must allow records to be retained beyond the retentions periods specified in Commission rules.*[8] [emphasis added]

2.2.2 Compliance Assessment

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

Reminder: This requirement is an alternative to the complete time-stamped audit-trail requirement, which is addressed in Section 2.1.

2.2.3 Amazon EBS Snapshot Capabilities

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

2.2.3.1 Overview

- Each Snapshot is a point-in-time archival copy (replica) of the source EBS Volume and provides a recovery point to reestablish the archived records stored by the Snapshot. The Snapshot source may be (a) a single EBS Volume or (b) an entire Amazon EC2 Instance, which captures a separate Snapshot of each EBS Volume attached to the Instance.
  - Note: A Data Lifecycle Manager (DLM) policy may be configured to create Snapshots at prescribed intervals. However, at the time of this report, the DLM configurations cannot apply *Snapshot Lock*.

---

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

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

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

- Records and associated record metadata are immutably stored in each Snapshot, i.e., point-in-time archival copy, which may be used to retrieve the associated records. Cohasset recommends records be stored within 24 hours of creation to minimize risk of records being changed or deleted prior to applying *Snapshot Lock* retention controls. In EBS, this is accomplished by:
  - Creating Snapshots every 24 hours, and
  - Setting the *Snapshot Lock* duration (i.e., the *Lock Expiry Timestamp*) that meets or exceeds the required retention period.
- The following table summarizes the *Snapshot Lock* retention controls applied in *Compliance* versus *Governance* modes. See the subsections below the following table, for information on how to configure the *Snapshot Lock* retention controls and details about the resulting integrated controls.

	***Snapshot Lock* retention controls, in highly-restrictive *Compliance* mode**	***Snapshot Lock* retention controls, in less-restrictive *Governance* mode**
Protecting record content and immutable metadata	• By design, the contents of a Snapshot cannot be modified for its stored lifespan. Therefore, the contents of the records and record metadata stored in the Snapshot cannot be modified for its stored lifespan. • The Snapshot ID, Snapshot Description, Snapshot creation timestamp, and Volume ID are immutable for the lifespan of the Snapshot.	
Restricting changes to *Snapshot Lock* retention controls	• For Snapshots set to highly-restrictive *Compliance* mode, *Snapshot Lock* retention controls cannot be unlocked (i.e., *Snapshot Lock* cannot be removed) and cannot be downgraded to *Governance* mode. • A Snapshot's *Lock Expiry Timestamp* cannot be reduced or removed, though it can be extended (lengthened). • Accordingly, *Compliance* mode assures *Snapshot Lock* retention controls are not circumvented by any user or process. • Note: During the *cooling-off* grace period, if set, *Snapshot Lock* retention controls can be changed or unlocked (i.e., *Snapshot Lock* can be removed).	• For Snapshots set to less-restrictive *Governance* mode, *Snapshot Lock* retention controls can be: ○ Unlocked (i.e., *Snapshot Lock* and *Lock Expiry Timestamp* can be removed), by users with the special identity and access management (IAM) permission of *UnlockSnapshot.* ○ Upgraded to highly-restrictive *Compliance* mode. • A Snapshot's *Lock Expiry Timestamp* can be extended (lengthened) and can be reduced. • Accordingly, procedural controls and monitoring are required to scrutinize user and administrator actions taken to unlock *Snapshot Lock* retention controls.
Applying and removing *legal holds*	• *Legal Hold* obligations are met by extending the *Lock Expiry Timestamp* for the Snapshot. • Note: Care must be taken, since the *Lock Expiry Timestamp* cannot be reduced by any user, when *Snapshot Lock* is set to *Compliance* mode.	• *Legal Hold* obligations are met by extending the *Lock Expiry Timestamp* for the Snapshot.
Restricting deletion of Snapshots	• Attempts by any user to **delete** a Snapshot prior to the expiration of the *Lock Expiry Timestamp* are rejected. • The *Snapshot Lock* retention controls cannot be unlocked or circumvented by any user or administrator. • See Section 2.2.3.4, *Deletion Controls*, for additional information.	• Attempts by standard users to **delete** a Snapshot, prior to the expiration of the *Lock Expiry Timestamp* are rejected. • Users with the special IAM permission of *LockSnapshot* are allowed to shorten the *Lock Expiry Timestamp* and users with the special IAM permission of *UnlockSnapshot* are allowed to unlock the Snapshot Lock retention controls to authorize premature deletion. • See Section 2.2.3.4, *Deletion Controls*, for additional information.

2.2.3.2 Record Object Definition and Controls

- Records and associated immutable record metadata are immutably stored in each Snapshot, i.e., point-in-time archival copy, which may be used to retrieve the associated records. Cohasset recommends records be stored within 24 hours of creation to minimize risk of records being changed or deleted prior to applying *Snapshot Lock* retention controls. In EBS, this is accomplished by:
  - Creating Snapshots every 24 hours, and
  - Setting the Snapshot's *Lock Expiry Timestamp* to meet or exceed the required retention period.
- By design, the contents of a Snapshot cannot be modified for the lifespan of the stored Snapshot. Therefore, the contents of the records and record metadata stored in the Snapshot cannot be modified for the lifespan of the stored Snapshot.
- The Snapshot's immutable metadata includes: (a) Snapshot ID (unique identifier), (b) Snapshot Description, (c) Volume ID of the Volume associated with the Snapshot, and (d) Snapshot creation timestamp.
- The Snapshot's mutable metadata includes: (a) Snapshot name, (b) encryption status, and (c) storage tier.
- *Snapshot Lock* controls may be modified only as described in the row entitled *Modifying or unlocking Snapshot Lock retention controls*, in the following table.
- To apply *Snapshot Lock* retention controls to a specific Snapshot, using one of the supported AWS Service Interfaces, authorized users apply the following settings.
  - Select the Snapshot to which *Snapshot Lock* will be applied.
  - Set to highly-restrictive *Compliance* mode or less-restrictive *Governance* mode. Reminder: Less-restrictive *Governance* mode requires procedural controls and monitoring to scrutinize user and administrator actions taken to unlock *Snapshot Lock* retention controls.
  - Set the Snapshot's *Lock Expiry Timestamp* by either:
    - Specifying an explicit *Lock Expiry Timestamp*, or
    - Specifying the lock duration (in days or years), within the allowable range of 1 and 36,500 days.
      - When the lock duration is provided, the *Lock Expiry Timestamp* is calculated and stored as Snapshot metadata.
        - When the Snapshot is in the *pending* state, (a) attempts to delete the Snapshot are blocked and (b) when the Snapshot transitions from *pending* to *completed* state, the lock duration is added to the Snapshot's completion timestamp to calculate the *Lock Expiry Timestamp*.
        - When the *Snapshot Lock* retention controls are set for a Snapshot in the *completed* state, the lock duration is added to the *LockCreatedOn* timestamp to calculate the *Lock Expiry Timestamp*.
  - When highly-restrictive *Compliance* mode is selected, a *cooling-off period* (between 0 and 72 hours) may be set. During the *cooling-off period*, authorized users may change or unlock the *Snapshot Lock* retention controls.

- The following table describes the integrated retention controls for non-rewriteable, non-erasable record format when *Snapshot Lock* is successfully applied to the Snapshot in either *Compliance* or *Governance* mode.

	***Snapshot Lock* retention controls, in highly-restrictive *Compliance* mode**	***Snapshot Lock* retention controls, in less-restrictive *Governance* mode**
Protecting record content and metadata	● Records are retained within the Snapshot, and each Snapshot is inherently read-only and unchangeable. Therefore, the record content, record names and other record metadata cannot be changed over the lifespan of the Snapshot. ● Each Snapshot is a point-in-time archival copy and, by design, cannot be overwritten or modified. ● The Snapshot ID, Snapshot Description, Snapshot creation timestamp, and Volume ID are immutable for the lifespan of the Snapshot, though the Snapshot Name may be changed.	
Modifying or unlocking *Snapshot Lock* retention controls	● For Snapshots set to highly-restrictive *Compliance* mode, users: ○ Cannot change *Compliance* to *Governance.* ○ Cannot *unlock* the *Snapshot Lock*, i.e., cannot remove *Snapshot Lock* and cannot remove the *Lock Expiry Timestamp.* ○ Can extend, but cannot reduce, the *Lock Expiry Timestamp*. Accordingly, *Compliance* mode assures *Snapshot Lock* retention controls are not circumvented by any user or process. ● For Snapshots set to *Compliance-cooloff* mode, authorized users: ○ Can change the *Snapshot Lock* retention controls (i.e., change from *Compliance-cooloff* to *Governance* and/or change the *Lock Expiry Timestamp*). ○ Can *unlock* (i.e., remove) the *Snapshot Lock* retention controls.	● For Snapshots set to less-restrictive *Governance* mode, users: ○ Can change *Governance* to *Compliance.* ○ Can *unlock* the *Snapshot Lock*, i.e., can remove *Snapshot Lock* and the *Lock Expiry Timestamp*. ○ Can extend or reduce the *Lock Expiry Timestamp*. Accordingly, procedural controls and monitoring are required to scrutinize user and administrator actions taken to unlock *Snapshot Lock* retention controls. ● Note: Only users with the special IAM permission of *LockSnapshot* may extend or reduce the *Lock Expiry Timestamp*. Additionally, only users with the special IAM permission of *UnlockSnapshot* can unlock the *Snapshot Lock* retention controls, i.e., can remove the *Snapshot Lock* state of *Governance* and remove the *Lock Expiry Timestamp.*
Restricting deletion of Snapshots	● Attempts by any user to **delete** a Snapshot prior to the expiration of the *Lock Expiry Timestamp* are rejected, ● The *Snapshot Lock* retention controls cannot be unlocked or circumvented by any user or administrator. ● See Section 2.2.3.4, *Deletion Controls*, for additional information.	● Attempts by standard users to **delete** a Snapshot, prior to the expiration of the *Lock Expiry Timestamp* are rejected. ● Users with the special IAM permission of *UnlockSnapshot* are allowed unlock the *Snapshot Lock* retention controls, which permits deletion by an authorized user or administrator. ● See Section 2.2.3.4, *Deletion Controls*, for additional information.
Copying Snapshots and associated records	● A Snapshot, and the records stored within it, can be copied (a) within the same AWS region, (b) across different regions and within the same AWS account, or (c) across AWS accounts. ○ The creation timestamp of the copy reflects the date and time that the copy operation was completed and is not the time when the source Snapshot was taken. ○ The Volume ID, which is tracked in the source Snapshot, is not populated in the metadata of the copy.	
Moving Snapshots and associated records	● Snapshots cannot be directly moved to a different AWS location. ● Additionally, Snapshots are inextricably linked to the source Volume and this link cannot be removed.	

	***Snapshot Lock* retention controls, in highly-restrictive *Compliance* mode**	***Snapshot Lock* retention controls, in less-restrictive *Governance* mode**
Displaying *Snapshot Lock* retention controls	● To aid the user, the following *Snapshot Lock* settings can be viewed in the Snapshot Settings tab of the AWS Management Console or using the *DescribeLockedSnapshots* API: ○ *Snapshot Lock* mode (i.e., *Compliance, Compliance-cooloff,* or *Governance*) ○ Locked date (i.e., timestamp when the *Snapshot Lock* settings were applied) ○ *Lock Expiry Timestamp* (i.e., date the *Snapshot Lock* retention controls expire) ○ *Cooling-off* end date (i.e., timestamp when the *Snapshot Lock Compliance* mode settings will apply, due to expiration of the cooling-off period)	
Accessing records	● To access the contents (records) stored within a Snapshot, first, the desired Snapshot is selected, then a new EBS Volume is created from the Snapshot and is attached to an Amazon EC2 Instance. Thereafter, the associated EC2 instance is utilized to mount the volume and access the records retained by the Snapshot. ● Also see Section 2.4, *Capacity to Download and Transfer Records and Location Information.*	
Tiering storage classes	● The incremental Snapshot is stored in the Standard tier. ● The *Snapshot Archive* feature converts the incremental Snapshot to a full Snapshot stored in the Archive tier. ● Note: Snapshots are stored on Amazon S3, however the S3 storage class cannot be specified.	

- *Snapshot Lock* retention controls may be unlocked, by users with the special IAM permission of *UnlockSnapshot*, as follows:
  - When the *Snapshot Lock* retention controls are in *Governance* mode, authorized users may unlock the *Snapshot Lock* retention controls.
  - During the *cooling-off period,* the *Snapshot Lock* retention controls are in *Compliance-cooloff* state and authorized users may unlock the *Snapshot Lock* retention controls.
- *Snapshot Lock* retention controls may be set by users with the IAM permission of *LockSnapshot*.

2.2.3.3 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 released.

- The *Lock Expiry Timestamp* may be extended for Snapshots that are subject to the hold. If the initial extension of the *Lock Expiry Timestamp* is insufficient, the *Lock Expiry Timestamp* must continue being extended to meet the legal hold timeframe.
- When the *Snapshot Lock* is set to *Compliance* mode, the *Lock Expiry Timestamp* cannot be reduced. Therefore, Cohasset recommends extending the *Lock Expiry Timestamp* in smaller increments to avoid excessive retention, after the legal hold is released.

2.2.3.4 Deletion Controls

- The following table summarizes how deletion eligibility is determined and the controls associated with deleting Snapshots and associated metadata, when the *Snapshot Lock* is set to *Compliance* or *Governance* modes.

	***Snapshot Lock* retention controls, in highly-restrictive *Compliance* mode**	***Snapshot Lock* retention controls, in less-restrictive *Governance* mode**
Determining eligibility for deletion	● A Snapshot, together with its metadata and the records retained within the Snapshot, is eligible for deletion when the following conditions are met: ○ The Snapshot's *Lock Expiry Timestamp* is in the past, and ○ *Snapshot Lock* is not in *Compliance-cooloff* mode.	
Deleting eligible Snapshots and associated records	● An eligible Snapshot can be deleted, either by a delete action taken by an authorized user or initiated by an associated Data Lifecycle Manager (DLM) policy. ● Note: The DLM policy will make one attempt to delete the Snapshot upon expiration of the age-based or count-based retention setting, which are separate from the *Snapshot Lock* retention controls. ○ If the *Snapshot Lock* retention controls allow deletion, the Snapshot is deleted. ○ If the *Snapshot Lock* retention controls are not yet expired, the deletion attempt is rejected. ▪ Subsequent efforts to delete the Snapshot must be initiated separate from the DLM policy.	
Using privileged delete	● Deletion of each Snapshot, and its associated immutable metadata, is prohibited until Snapshot's *Lock Expiry Timestamp* is in the past. ○ When set to *Compliance* mode, the *Snapshot Lock* retention controls cannot be unlocked or circumvented by any user or administrator. ● During the *cooling-off period*, the *Snapshot Lock* is in *Compliance-cooloff* state, which allows the *Snapshot Lock* retention controls to be unlocked; thereafter, the Snapshot may be deleted by authorized users.	● For standard users, deletion of each Snapshot and its associated immutable metadata are prohibited until Snapshot's *Lock Expiry Timestamp* is in the past. ● Users with the special IAM permission of *UnlockSnapshot* can unlock the *Snapshot Lock* retention controls before the *Lock Expiry Timestamp* is in the past. Unlocked Snapshots may be deleted by an authorized user or administrator. Accordingly, procedural controls and monitoring are required to scrutinize user and administrator actions taken to unlock *Snapshot Lock* retention controls.
Applying the optional Recycle Bin feature	● Optionally, as a separate data recovery feature to help protect business-critical data against accidental or malicious deletion, Recycle Bin can be enabled by configuring separate Recycle Bin retention rules. ● A Recycle Bin retention rule can be configured to apply to a certain tag assigned to resources (e.g., Snapshot) or to a region. Each rule specifies: ○ Resource type (e.g., Snapshots) to retain in the Recycle Bin, after deletion from the original storage location. ○ Duration of time (between one day and one year) to retain the resource (e.g., Snapshot) in the Recycle Bin before permanent deletion. ● While the resource (e.g., Snapshot) is in the Recycle Bin, it can be restored, at any time. ● When the applied Recycle Bin retention period expires, the resource is automatically deleted. ● Optionally, administrators may set an *Unlock Delay Period* (between 7 to 30 days) when locking a Recycle Bin retention rule. ○ If a *Locked* Recycle Bin retention rule is unlocked, it will be in a *Pending Unlock* state until the *Unlock Delay Period* expires. While in the *Pending Unlock* state, records (e.g., Snapshots) are retained in the Recycle Bin, as if the retention rule was *Locked*. This disallows premature removal of Snapshots from the Recycle Bin, during the *Unlock Delay Period*, providing time to correct malicious unlocking actions. ○ *Locked* Recycle Bin retention rules cannot be modified or deleted by any user, and resources (e.g., Snapshots) cannot be removed from the Recycle Bin, except when the Recycle Bin retention period expires.	

2.2.3.5 Security

- Amazon Web Services are designed to meet enterprise security and compliance requirements.
- Access to Amazon EBS Snapshots requires credentials, which must have permissions to access AWS resources, such as EBS Volumes.
- The regulated entity may configure AWS server-side encryption, using AWS Key Management Service to prevent unauthorized access of the data.
- Optionally, in addition to setting the *Lock Expiry Timestamp*, the regulated entity may configure and *Lock* its Recycle Bin retention rules to help protect business-critical data against accidental or malicious deletion.

2.2.3.6 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 EBS system clocks regularly and frequently check the time of the external source and resynchronize. Neither end users nor system administrators have the ability to manipulate system time. These controls prevent or correct any inadvertent or intentional administrative modifications of the time clock, which could allow for premature deletion of Snapshots.

2.2.4 Additional Considerations

In addition, for this requirement, the regulated entity is responsible for:

- Creating Snapshots at intervals required to capture the records retained within the Snapshot and setting an appropriate Snapshot *Lock Expiry Timestamp*.
  - Cohasset recommends that Snapshots, containing required records, be created within 24 hours to help assure accurate and complete records are captured. Subsequent Snapshots may include prior day's records; however, the longer timespan from record creation to Snapshot creation may result in the Snapshot containing records that have been changed or missing records that have been deleted.
- Storing Snapshots containing records requiring event-based[10] retention periods in a separate compliant system, since Amazon EBS Snapshot features do not currently support event-based retention periods.
- Extending the *Lock Expiry Timestamp,* to preserve Snapshots needed for legal matters, government investigations, external audits and other similar circumstances.
- Monitoring Snapshots that are created using a DLM policy and also have *Snapshot Lock* retention controls applied to ensure that deletion occurs as expected. Reminder: the DLM policy will attempt deletion when its age-based or count-based retention settings expire. If the *Lock Expiry Timestamp* is not in the past, the deletion attempt by the DLM policy will be rejected and the DLM policy will not make any subsequent attempts to delete the Snapshot.

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

- Configuring AWS server-side encryption, using AWS Key Management Service, or employing a different method of preventing unauthorized access of the data.

Additionally, the regulated entity is responsible for: (a) maintaining its account in good standing and paying for appropriate services to allow records to be retained until the applied retention periods and holds have expired or until the records have been transferred to other compliant storage, (b) authorizing user privileges, and (c) maintaining appropriate technology, encryption keys, and other information and services needed to retain 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 EBS Snapshots meets this SEC requirement for complete and accurate recording of records and post-recording verification processes, when the considerations identified in Section 2.3.4 are satisfied.

2.3.3 Amazon EBS Snapshot Capabilities

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

2.3.3.1 Recording Process

- Amazon EBS utilizes advanced electronic recording technology which applies a combination of checks and balances to assure that Snapshots are created in a high quality and accurate manner.
- When the Snapshot is fully written, its state changes from *pending* to *completed*; thereafter, the *Snapshot Lock* controls are applied.
  - Snapshots are often created within a few minutes; however, the initial Snapshot and Snapshots capturing significant changes require longer periods to fully write and the state to change to *completed*.
- During the Snapshot creation process, the integrity of the data is validated using checksums.

2.3.3.2 Post-Recording Verification Process

- Snapshots are automatically saved to Amazon S3 for long-term retention. S3 is designed for 11-nines of durability, ensuring Snapshots are highly available.
- AWS regularly verifies the integrity of data stored using checksums. If AWS detects data loss, it is repaired using redundant data.

- AWS also calculates checksums on all network traffic to detect corruption of data packets when storing or retrieving data.

2.3.4 Additional Considerations

- The source system is responsible for storing the complete contents of required records in EBS Volumes. Amazon EBS Snapshot assures the accurate capture and recording processes of snapshots of EBS Volumes.

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 EBS Snapshots meets this SEC requirement to maintain the capacity to readily download and transfer the records and information used to locate the records, when the considerations described in Section 2.4.4 are satisfied.

2.4.3 Amazon EBS Snapshot Capabilities

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

- Amazon EBS assures that the hardware and software capacity allows for ready access to Snapshots and the associated records. Further, Snapshots are automatically saved to Amazon S3 for long-term retention. S3 is designed for 11-nines of durability and 99.99% availability over a given year, ensuring the high availability of Snapshots.
- Each Snapshot is a virtual point-in-time archival copy of an EBS Volume and is:
  - Inextricably linked to the source EBS Volume that was copied; this ensures findability.

- Separately identified by immutable metadata, including: (a) Snapshot ID, (b) Snapshot Description, (c) Volume ID (i.e., identifier of the Volume associated with the Snapshot), and (d) Snapshot creation timestamp.
- Organized consistent with the source, i.e., the Snapshot contents are a point-in-time replica of the associated source EBS Volume.

- Additionally, the following *Snapshot Lock* settings can be viewed in the *Snapshot Settings tab* of the AWS Management Console or using the *DescribeLockedSnapshots* API:
  - *Snapshot Lock* mode (i.e., *Compliance*, *Compliance-cooloff,* or *Governance*).
  - Locked date (i.e., timestamp when the *Snapshot Lock* settings were applied).
  - *Lock Expiry Timestamp* (i.e., date the *Snapshot Lock* retention controls expire).
  - *Cooling-off* end date (i.e., timestamp when the *Snapshot Lock Compliance* mode settings will apply, due to expiration of the cooling-off period that was set).
- To access the contents (i.e., the records and associated record metadata) stored within a Snapshot, first the desired Snapshot is selected, then a new EBS Volume is created from the Snapshot and attached to an Amazon EC2 Instance. Thereafter, the associated EC2 Instance is utilized to mount the Volume.
  - The records and associated record metadata retained by the Snapshot can be accessed using EC2 tools.
  - The records and associated record metadata can be extracted using local tools to render a human readable view and produce the records in the requested electronic format.

2.4.4 Additional Considerations

In addition, for this requirement, the regulated entity is responsible for: (a) maintaining its account in good standing, (b) authorizing user privileges, and (c) maintaining appropriate technology and resource capacity, encryption keys, and other information and services needed to use Amazon EBS Snapshots 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 promulgate 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.[11] [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.[12] [emphasis added]

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

2.5.2 Compliance Assessment

Cohasset upholds that the functionality of Amazon EBS Snapshots meets the requirement in SEC Rules 17a-4(f)(2)(v)(B) and 18a-6(f)(2)(v)(B) by retaining a persistent alternate source to reestablish the records, when the considerations described in Section 2.5.4 are satisfied.

2.5.3 Amazon EBS Snapshot Capabilities

For compliance with paragraph (B), Snapshots are automatically stored in S3, with 11-nines of durability.

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

2.5.4 Additional Considerations

In addition, for compliance with 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 EBS Snapshots and permit access to the records.

[11] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66421.

[12] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66421.

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 EBS Snapshots (optionally, in conjunction with enabling CloudTrail) supports the regulated entity's efforts to meet this SEC audit system requirement.

2.6.3 Amazon EBS Snapshot Capabilities

The regulated entity is responsible for and AWS supports compliance with this requirement for an audit system.

- A Snapshot is created (input) by identifying a virtual point-in-time archival copy of an EBS Volume. Each created (input) Snapshot is:
  - Separately identified by immutable metadata, including: (a) Snapshot ID, (b) Snapshot Description, (c) Volume ID (i.e., the identifier of the Volume associated with the Snapshot), and (d) Snapshot creation timestamp.
  - Organized consistent with the source, i.e., the Snapshot contents are a point-in-time replica of the associated source EBS Volume.
- Inputting of record modifications is prohibited.
  - By design, the contents of a Snapshot cannot be modified for the lifespan of the stored Snapshot. Therefore, the contents of the records and record metadata stored in the Snapshot cannot be modified for the lifespan of the stored Snapshot.
- In addition to the immutable record metadata, at the regulated entity's option, Amazon EBS Snapshot activities are integrated with the AWS CloudTrail service.
  - AWS CloudTrail is enabled on AWS accounts, by default.

- AWS CloudTrail captures a record (an event history) of Amazon EBS Snapshot events (i.e., actions taken by a user, role, or AWS service) and the date of each event. The event history is:
  - Viewable, searchable, and downloadable.
  - Stored for 90 days.
- CloudTrail events may be exported via supported integrations with external applications such as security information and event management tools.

2.6.4 Additional Considerations

The regulated entity is responsible for maintaining an audit system for inputting Snapshots and its associated records. In addition to relying on the immutable metadata, the regulated entity may utilize EBS Snapshot metadata alone or in conjunction with CloudTrail and a security information and event management tool.

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

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

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

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

> *The proposed amendments to Rules 17a-4 and 18a-6 and the [CFTC] principles-based approach recommended by the commenters share an objective: ensuring the authenticity and reliability of regulatory records. However, the audit-trail requirement is more likely to achieve this objective because, like the existing WORM requirement, it sets forth a specific and testable outcome that the electronic recordkeeping system must achieve: the ability to access and produce modified or deleted records in their original form.*[13] [emphasis added]

In Section 2 of this report, Cohasset assesses the *Snapshot Lock* retention controls set to:

- *Compliance mode*, a highly-restrictive option, which provides strict retention and deletion prevention controls, or
- *Governance mode,* a less-restrictive option, which allows authorized administrators to reduce the *Lock Expiration Timestamp* or unlock *Snapshot Lock* retention controls, therefore, administrative procedures and monitoring are required to ensure compliant retention controls remain applied.

See subsection 2.2.3.1, *Overview*, for a summary of *Snapshot Lock* retention controls for *Compliance* and *Governance* mode options.

In the following table, Cohasset correlates the functionality of Amazon EBS Snapshots, using *Snapshot Lock*, with the *principles-based* CFTC requirements related to the *form and manner of retention* and the *inspection and production of regulatory records*. The first column enumerates the CFTC regulation. The second column provides Cohasset's analysis and opinion regarding the ability of Amazon EBS Snapshots to meet the requirements for electronic regulatory records in CFTC Rule 1.31(c)-(d).

[13] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.

CFTC 1.31(c)-(d) Regulation [emphasis added]	**Compliance Assessment Relative to CFTC 1.31(c)-(d)**
(c) Form and manner of retention. Unless specified elsewhere in the Act or Commission regulations in this chapter, all regulatory records must be created and retained by a records entity in accordance with the following requirements: *(1) Generally. Each records entity shall retain regulatory records in a form and manner that ensures the authenticity and reliability of such regulatory records in accordance with the Act and Commission regulations in this chapter.* *(2) Electronic regulatory records. Each records entity maintaining electronic regulatory records shall establish appropriate systems and controls that ensure the authenticity and reliability of electronic regulatory records, including, without limitation:* *(i) Systems that maintain the security, signature, and data as necessary to ensure the authenticity of the information contained in electronic regulatory records and to monitor compliance with the Act and Commission regulations in this chapter;*	It is Cohasset's opinion that the CFTC requirements in (c)(1) and (c)(2)(i), for records[14] with time-based retention periods, are met by the functionality of Amazon EBS Snapshots, with *Snapshot Lock* in either *Compliance* or *Governance* mode, as described in: ● 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] Snapshots retain immutable metadata attributes 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. The immutable metadata attributes include the following: ● Snapshot ID (unique identifier) ● Snapshot Description ● Volume ID, which identifies the Volume associated with each completed Snapshot ● Snapshot creation timestamp Additionally, mutable metadata attributes stored for Snapshots include Snapshot Name and retention controls. The most recent values of mutable metadata are retained for the same time period as the associated records.
(ii) Systems that ensure the records entity is able to produce electronic regulatory records in accordance with this section, and ensure the availability of such regulatory records in the event of an emergency or other disruption of the records entity's electronic record retention systems; and	It is Cohasset's opinion that Amazon EBS Snapshot capabilities to retain a persistent alternate source to reestablish the records and associated system metadata, as described in Section 2.5, *Record Redundancy*, 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*.

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

CFTC 1.31(c)-(d) Regulation [emphasis added]	**Compliance Assessment Relative to CFTC 1.31(c)-(d)**
(iii) The creation and maintenance of an up-to-date inventory that identifies and describes each system that maintains information necessary for accessing or producing electronic regulatory records.	The regulated entity is required to create and retain an *up-to-date inventory*, as required for compliance with 17 CFR § 1.31(c)(iii).
(d) Inspection and production of regulatory records. Unless specified elsewhere in the Act or Commission regulations in this chapter, a records entity, at its own expense, must produce or make accessible for inspection all regulatory records in accordance with the following requirements: *(1) Inspection. All regulatory records shall be open to inspection by any representative of the Commission or the United States Department of Justice.* *(2) Production of **paper** regulatory records. **** *(3) Production of **electronic** regulatory records.* *(i) A request from a Commission representative for electronic regulatory records will specify a reasonable form and medium in which a records entity must produce such regulatory records.* *(ii) A records entity must produce such regulatory records in the form and medium requested promptly, upon request, unless otherwise directed by the Commission representative.* *(4) Production of **original** regulatory records. ****	It is Cohasset's opinion that Amazon EBS Snapshots 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 EBS Snapshots[15] 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 EBS Snapshots, when properly configured, has the following functionality, which meets the regulatory requirements:

- Retains Snapshots in non-rewriteable, non-erasable format for time-based retention periods by applying *Snapshot Lock* retention controls set to highly-restrictive *Compliance* mode or less-restrictive *Governance* mode. Each Snapshot is point-in-time archival copy and recovery point to reestablish both (a) the archived records and (b) the associated immutable record metadata stored in the Snapshot.
- Allows the *Lock Expiry Timestamp* (i.e., the date the *Snapshot Lock* retention controls expire) to be extended to retain records for regulatory compliance or preserve records for a legal hold.
- Prohibits deletion of records until the *Snapshot Lock* retention controls expire.
- Verifies the accuracy of the process for storing and retaining Snapshots which immutably store records and associated record metadata.
- Provides authorized users with the capacity and tools to readily locate and restore Snapshots, then access the restored Snapshots to find and download the records and information needed to locate the records for a browser or other local tool to render a human readable view and produce it in the requested electronic format.
- Provides redundancy processes for either retrieving an accurate replica or regenerating an accurate replica of the Snapshot and associated records should an error occur or an availability problem be encountered.
- Supports the regulated entity's obligation to retain an audit system for non-rewriteable, non-erasable records.

Accordingly, Cohasset concludes that Amazon EBS Snapshots, 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).

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

Appendix A • Overview of Relevant Electronic Records Requirements

This section establishes the context for the regulatory requirements that are the subject of this assessment by providing an overview of the regulatory foundation for electronic records retained on compliant electronic recordkeeping systems.

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

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

Effective January 3, 2023, the U.S. Securities and Exchange Commission (SEC) promulgated amendments[16] to 17 CFR § 240.17a-4 (Rule 17a-4) and 17 CFR § 240.18a-6 (Rule 18a-6), which define more technology-neutral requirements for electronic recordkeeping systems.

> *The objective is to prescribe rules that remain workable as record maintenance and preservation technologies evolve over time but also to set forth requirements designed to ensure that broker-dealers and SBS Entities maintain and preserve records in a manner that promotes their integrity, authenticity, and accessibility.*[17] [emphasis added]

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

> *Under the final amendments, broker-dealers and nonbank SBS Entities have the flexibility to preserve all of their electronic Broker-Dealer Regulatory Records or SBS Entity Regulatory Records either by: (1) using an electronic recordkeeping system that meets either the audit-trail requirement or the WORM requirement; or (2) preserving some electronic records using an electronic recordkeeping system that meets the audit-trail requirement and preserving other electronic records using an electronic recordkeeping system that meets the WORM requirement.*[18] [emphasis added]

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

A.1.1 Record and Audit-Trail Alternative

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

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

[17] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66428.

[18] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66419.

> *[T]o preserve Broker-Dealer Regulatory Records and SBS Regulatory Records, respectively, on the same electronic recordkeeping system they use for business purposes, but also to require that the system have the capacity to recreate an original record if it is modified or deleted. This requirement was designed to provide the same level of protection as the WORM requirement, which prevents records from being altered, over-written, or erased.*[19] [emphasis added]

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

> *[L]ike the existing WORM requirement, [the audit-trail requirement] sets forth a specific and testable outcome that the electronic recordkeeping system must achieve: the ability to access and produce modified or deleted records in their original form.*[20] [emphasis added]

Further, the audit-trail applies only to required records: *"the audit-trail requirement applies to the final records required pursuant to the rules, rather than to drafts or iterations of records that would not otherwise be required to be maintained and preserved under Rules 17a-3 and 17a-4 or Rules 18a-5 and 18a-6."*[21] [emphasis added]

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

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

> *The Commission confirms that a broker-dealer or nonbank SBS Entity can rely on the 2003 and 2019 interpretations with respect to meeting the WORM requirement of Rule 17a-4(f) or 18a- 6(e), as amended.*
> *****
> *In 2001, the Commission issued guidance that Rule 17a-4(f) was consistent with the ESIGN Act. The final amendments to Rule 17a-4(f) do not alter the rule in a way that would change this guidance. Moreover, because Rule 18a-6(e) is closely modelled on Rule 17a-4(f), it also is consistent with the ESIGN Act****[22] [emphasis added]

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

- *Commission Guidance to Broker-Dealers on the Use of Electronic Storage Media Under the Electronic Signatures in Global and National Commerce Act of 2000 With Respect to Rule 17a-4(f), Exchange Act Release No. 44238 (May 1, 2001), 66 FR 22916 (May 7, 2001)* (2001 Interpretative Release).
- *Electronic Storage of Broker-Dealer Records, Exchange Act Release No. 47806 (May 7, 2003), 68 FR 25281, (May 12, 2003)* (2003 Interpretative Release).
- *Recordkeeping and Reporting Requirements for Security-Based Swap Dealers, Major Security Based Swap Participants, and Broker-Dealers, Exchange Act Release No. 87005 (Sept. 19, 2019), 84 FR 68568 (Dec. 16, 2019)* (2019 SBSD/MSBSP Recordkeeping Adopting Release).

---

19 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.
20 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.
21 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66418.
22 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66419.

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

> *A broker-dealer would not violate the requirement in paragraph* [(f)(2)(i)(B) (refreshed citation number)] *of the rule if it used an electronic storage system that prevents the overwriting, erasing or otherwise altering of a record during its required retention period through the use of integrated hardware and software control codes.*[23] [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.*[24] [emphasis added]

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

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

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

> *[A] broker-dealer must take appropriate steps to ensure that records are not deleted during periods when the regulatory retention period has lapsed but other legal requirements mandate that the records continue to be maintained, and the broker-dealer's storage system must allow records to be retained beyond the retentions periods specified in Commission rules.*[25] [emphasis added]

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

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

Financial Industry Regulatory Authority (FINRA) rules regulate member brokerage firms and exchange markets. Additionally, FINRA adopted amendments clarifying the application of FINRA rules to security-based swaps (SBS).[26]

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.*

---

23 2003 Interpretative Release, 68 FR 25282.

24 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).

25 2003 Interpretative Release, 68 FR 25283.

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

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

Effective August 28, 2017, the Commodity Futures Trading Commission (CFTC) amended 17 CFR § 1.31 (CFTC Rule) to modernize and make technology-neutral the form and manner in which to keep regulatory records. This resulted in less-prescriptive, principles-based requirements.

> *Consistent with the Commission's emphasis on a less-prescriptive, principles-based approach, proposed § 1.31(d)(1) would rephrase the existing requirements in the form of a general standard for each records entity to retain all regulatory records in a form and manner necessary to ensure the records' and recordkeeping systems' authenticity and reliability.*[27] [emphasis added]

The following definitions in 17 CFR § 1.31(a) confirm that recordkeeping obligations apply to all *records entities* and all *regulatory records*. Further, for *electronic regulatory records*, paragraphs (i) and (ii) establish an expanded definition of an electronic regulatory record to include information describing data necessary to access, search and display records, as well as information describing how and when such books and records were created, formatted, or modified.

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

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

> *Duration of retention. Unless specified elsewhere in the Act or Commission regulations in this chapter:*
>
> *(1) A records entity shall keep regulatory records of any swap or related cash or forward transaction (as defined in § 23.200(i) of this chapter), other than regulatory records required by § 23.202(a)(1) and (b)(1)-(3) of this chapter, from the date the regulatory record was created until the termination, maturity, expiration, transfer, assignment, or novation date of the transaction and for a period of not less than five years after such date.*
>
> *(2) A records entity that is required to retain oral communications, shall keep regulatory records of oral communications for a period of not less than one year from the date of such communication.*
>
> *(3) A records entity shall keep each regulatory record other than the records described in paragraphs (b)(1) or (b)(2) of this section for a period of not less than five years from the date on which the record was created.*
>
> *(4) A records entity shall keep regulatory records exclusively created and maintained on paper readily accessible for no less than two years. A records entity shall keep electronic regulatory records readily accessible for the duration of the required record keeping period.* [emphasis added]

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

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

Appendix B • Cloud Provider Undertaking

B.1 Compliance Requirement

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

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

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

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

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

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]

agreed to in the Traditional Undertaking. Rather, it means that the third party undertakes to provide to the Commission 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.[28] [emphasis added]

B.2 Amazon Undertaking Process

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

- The undertaking requires actions be taken by both parties:
  1. The regulated entity affirms 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 in Amazon EBS Snapshots, and
     - Consents to Amazon fulfilling the obligations set forth in this undertaking.
  2. Amazon:
     - Acknowledges that the records are the property of the regulated entity,
     - For the duration of the undertaking, agrees to facilitate within its ability, and not impede or prevent, the examination, access, download, or transfer of the records by a regulatory or trustee, as permitted under the law, and
     - Prepares the undertaking, utilizing the explicit language in the Rule, then submits, via email, the undertaking to the SEC.
- IMPORTANT NOTE: While Amazon provides this undertaking to the SEC on behalf of the regulated entity, the regulated entity is not relieved from its responsibility to prepare and maintain required records.

B.3 Additional Considerations

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

[28] 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.