Cohasset Associates

Amazon FSx for NetApp ONTAP

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 FSx for NetApp ONTAP (FSx for ONTAP) is a fully-managed AWS service that provides reliable, scalable, high-performance file storage built on NetApp's ONTAP file system.

In this report, Cohasset Associates, Inc. (Cohasset) assesses the functionality of FSx for ONTAP (see Section 1.3, *FSx for ONTAP 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 FSx for ONTAP, when properly configured and used with the *SnapLock* feature in *Compliance* mode, 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 FSx for ONTAP 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.

July 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 FSx for NetApp ONTAP 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 Section 5.1, *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 Section 5.3, *Overview of CFTC Rule 1.31(c)-(d) Electronic Regulatory Records Requirements*.

1.2 Purpose and Approach

To obtain an independent and objective assessment of the compliance capabilities of FSx for ONTAP 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 FSx for ONTAP, 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 FSx for ONTAP; 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 FSx for ONTAP and its functionality or other Amazon or NetApp products or services. The information utilized by Cohasset to conduct this assessment consisted of: (a) oral discussions, (b) system documentation, (c) user and system administrator guides, and (d) related materials provided by Amazon or obtained from publicly available resources.

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

1.3 FSx for ONTAP Overview and Assessment Scope

1.3.1 FSx for ONTAP Overview

Amazon Web Services (AWS) is a secure cloud services platform hosted by Amazon to provide modular cloud-based products and services. Amazon FSx for NetApp ONTAP (FSx for ONTAP) is a fully-managed AWS service that provides reliable, scalable, high-performance file[4] storage built on NetApp's ONTAP file system. FSx for ONTAP is broadly accessible from Linux, Windows, and macOS compute instances, whether running in AWS or on premises.

SnapLock is a feature of NetApp ONTAP and offers two retention modes for managing electronic records: *SnapLock Enterprise* and *SnapLock Compliance*. Evaluated in this assessment, *SnapLock Compliance* is designed to meet the stringent securities industry requirements for preserving records in a non-rewriteable, non-erasable format. FSx for ONTAP, when utilized with *SnapLock Compliance,* applies integrated control codes to prevent stored records from being modified, overwritten or deleted until the specified retention period has expired and any legal holds have been released.

The FSx for ONTAP storage architecture is depicted in figure 1 and key components are described below:

An **AWS Customer Account** provides a virtual private cloud (VPC) environment for secure, controlled access by the regulated entity to AWS resources. One or more FSx for ONTAP File Systems, may be contained within a single AWS Customer Account.

Each **FSx for ONTAP File System** is analogous to an ONTAP *Cluster* in on-premises deployments. A file system offers two types of physical storage tiers:

- **Primary Tier** – high performance solid-state drive storage, designed for active data.
- **Capacity Tier** – lower-cost, fully elastic storage tier optimized for infrequently accessed data.

The regulated entity has no direct access to storage drives for either tier, but rather, has access to a logical abstraction of the mapped storage.

A **Storage Virtual Machine (SVM)** is an isolated virtual file server, with its own endpoint IP address that provides client access to a subset of the ONTAP file system for administrative actions and to access stored data. SVMs provide secure, logical partitioning within the file system, for purposes of performance and/or

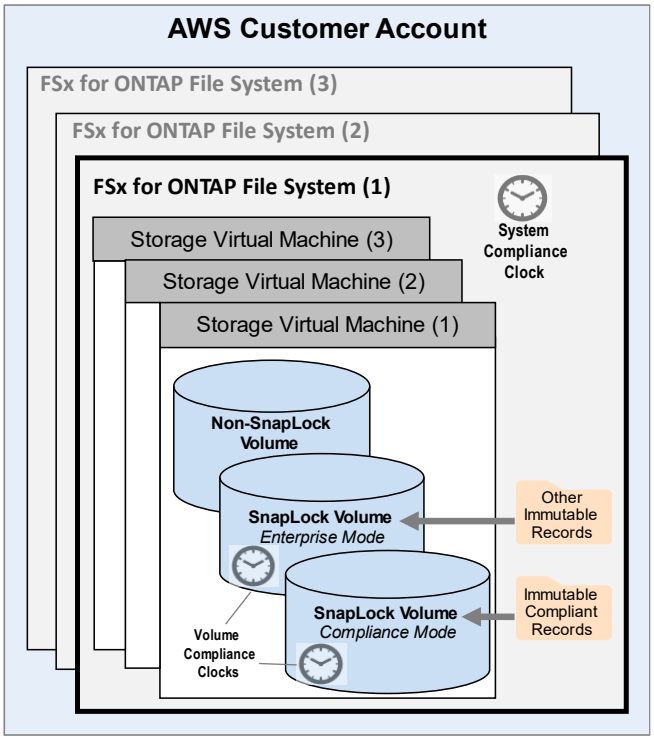

Figure 1: Logical storage architecture of FSx for ONTAP

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

security (e.g., separate departments and divisions). One or more SVMs may be contained within a single ONTAP file system.

Volumes are logical containers within SVMs that are responsible for storing files and directories. Policies established at the Volume level determine how much data can be stored and when policy-based tiering to Capacity Tier storage is to occur. For Volumes intended to store required records, (a) the Volume must be a FlexVol (i.e., standard) Volume and (b) the *SnapLock* feature must be configured and set to *Compliance* retention mode (hereinafter referred to as *SnapLock Compliance* Volumes) for compliance with the Rule. Note: *SnapLock Compliance*, SnapLock Enterprise, and non-SnapLock Volumes can coexist within a single SVM. Only *SnapLock Compliance* Volumes are assessed for compliance with the Rules.

1.3.2 Assessment Scope

The scope of this assessment is focused specifically on the compliance-related capabilities of Amazon FSx for NetApp ONTAP, with the *SnapLock* feature enabled on FlexVol Volumes and the retention mode set to *Compliance*.

This assessment excludes (a) FlexGroup Volumes (scale-out containers comprised of multiple FlexVol Volumes) and (b) AWS infrastructure running on-premises with AWS Outposts.

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 FSx for NetApp ONTAP, for compliance with the electronic recordkeeping system requirements promulgated in SEC Rules 17a-4(f)(2) and 18a-6(e)(2), as well as describing 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 FSx for ONTAP
- ***FSx for ONTAP 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 FSx for ONTAP, as described in Section 1.3, *FSx for ONTAP Overview and Assessment Scope*, relative to the enumerated requirements of SEC Rules 17a-4(f) and 18a-6(e).

2.1 Record 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 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 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 the complete time-stamped record audit-trail requirement promotes the authenticity and reliability of the records while providing flexibility, 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 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 FSx for ONTAP in comparison to this requirement of the SEC Rules.

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

Reminder: This record audit-trail 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 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 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*

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

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

> *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 FSx for ONTAP, with *SnapLock Compliance*, meets this SEC requirement to retain records in non-rewriteable, non-erasable format for the applied time-based[9] and event-based[10] 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 FSx for ONTAP Capabilities

This section describes the functionality of FSx for ONTAP 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

- FSx for ONTAP offers two *SnapLock* retention modes for use when storing records in a SnapLock Volume: *SnapLock Enterprise* and *SnapLock Compliance*. Evaluated in this assessment, *SnapLock Compliance* is designed to meet the stringent securities industry requirements for preserving records in a non-rewriteable, non-erasable format.
- Once the *SnapLock* retention mode for a storage Volume is set to *Compliance* (*SnapLock Compliance* Volume), the mode cannot be changed or removed, and stringent retention protection and record management controls are employed.

---

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.

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.

- To apply time-based or event-based retention controls to *files*, either (a) the source system must transmit explicit retention attributes or (b) the Default Retention Period and Autocommit features must be properly configured for the *SnapLock Compliance* Volume to apply default values if retention attributes are not provided by the source system.
- To apply time-based retention controls to *snapshots* of Volumes (i.e., a point-in-time copy of one or more Volumes), retention controls are provided by a SnapMirror Policy, defined using the *SnapLock for SnapVault* feature.
- When retention controls are applied to a record within a *SnapLock Compliance* Volume, integrated control codes are applied which:
  - Disable all write privileges for the content of the record, thus protecting it against modification or overwrite for the specified retention period.
  - Prohibit deletion of the record content and associated metadata until the assigned retention period expires and any legal holds are removed.
  - Prohibit the *shortening* of the retention period assigned to the record. However, the retention period may be extended for any record, as necessary, except while a legal hold is in effect.
  - Prohibit the deletion of the *SnapLock Compliance* Volume until all stored records are past their assigned retention period and deleted from the Volume.
  - Prohibit renaming a record or directory, which could hide the file or access path.
  - Prohibit use of *Privileged Delete*. (This command is not allowed for *SnapLock Compliance* Volumes.)

2.2.3.2 Required Configurations and Supported Protocols

To meet the requirements of the Rule, the following basic administrative setup must be completed:

- An FSx for ONTAP **file system** is created within the regulated entity's AWS Customer Account. As part of the file system creation process:
  - FSx automatically (a) enables encryption using AWS Key Management System (KMS) and (b) enables security policies which define the specific actions allowed within the file system.
  - A single Storage Virtual Machine (SVM) with a single root Volume is automatically created. Additional SVMs and data storage Volumes must be created separately.
- **Volumes** that will store required records are configured as follows:
  - The *SnapLock Compliance* retention mode must be enabled, which makes the Volume ***capable*** of retaining records in a non-rewriteable, non-erasable format for a designated retention period. Once *SnapLock Compliance* has been configured for a Volume, the retention mode cannot be changed or removed, and the Volume cannot be renamed. Note: *SnapLock Compliance* must be configured when a Volume is first created as SnapLock Enterprise Volumes and non-SnapLock Volumes cannot be converted to *SnapLock Compliance*.
  - Optionally, the following Volume configurations may be enabled, based on the needs of the regulated entity:

- *Auto-sizing* allows for the automatic expansion of the Volume's storage capacity to accommodate data writes.
- *Auto-tiering* automatically migrates data from Primary Tier to Capacity Tier storage, after a defined cooling period (i.e., the number of days that must elapse before data is tiered to lower-cost storage).

- The following optional *SnapLock Compliance* properties, when properly configured for a *SnapLock Compliance* Volume, offer additional guardrails for applying retention controls to records.
  - Default Retention Period: The Default Retention Period value (specified in terms of seconds, minutes, hours, days, months, or years) is used to compute a retention expiration date for the record if the source system sets the file to read-only but does not send an explicit retention expiration date or specify an event-based retention policy. *Note: The initial Default Retention Period for a Volume is automatically set to the same value as the Minimum Retention Period but may be changed at any time*.
  - Autocommit: The Autocommit capability, when enabled on a *SnapLock* Volume, is utilized when a file[11] is transmitted without a *read-only* attribute (with or without a retention expiration date). The record is automatically written to immutable storage using the Default Retention Period to calculate the retention expiration date. *Note: There are certain circumstances which result in the Minimum Retention Period being applied rather than the Default Retention Period. Care should be taken to assure the most appropriate retention value is applied.*
    - When Autocommit is configured for a *SnapLock Compliance* Volume, an Autocommit-period (i.e., wait period) must be set with a duration ranging between 5 minutes and 10 years. The record will be automatically committed to WORM storage if the content of the record has not been modified within the designated Autocommit-period.

    Note: If Autocommit and a Default Retention Period are not set for a Volume and a file is transmitted without explicit retention controls, it will be written to the Volume without retention controls and, therefore, will not be stored in compliance with the non-rewriteable, non-erasable requirements of the Rule.
  - Volume Append Mode (VAM) may be enabled for a *SnapLock Compliance* Volume that will store records that require additional content to be added over time, such as logging data, audio, or video files. This configuration assures that new files stored to the Volume are set to WORM-appendable, by default. *Note: the VAM setting can only be enabled on empty Volumes. (*See Section *2.2.3.3 Records and Retention Controls,* for more details regarding WORM-appendable records.)
  - Minimum[12] and Maximum[13] retention periods may be set for each *SnapLock Compliance* Volume. These Minimum and Maximum parameters are utilized during the initial recording of a record, when an explicit retention expiration date is supplied by the source system, to ensure the supplied date falls within the allowable range.

[11] See Section 2.2.3.3 *Record Definition and Retention Control*, for the types of files, which include both standard and WORM-appendable files.

[12] The Minimum retention period defaults to zero but may be increased.

[13] The Maximum retention period defaults to 30 years but may be increased up to 100 years.

- Transmission of records and ongoing maintenance of the FSx for ONTAP environment is accomplished via a combination of the following protocols and management tools:
  - NFS and SMB/CIFS protocols.
  - AWS management tools such as AWS Management Console, AWS CLI (command line interface), Amazon FSx APIs (application programming interfaces) and SDKs (software development kits), and AWS CloudFormation.
  - NetApp management tools such as ONTAP CLI and ONTAP REST APIs (or tools built on these APIs).

2.2.3.3 Record Definition and Retention Controls

- Three types of records are supported by *SnapLock*:
  1. Standard file: Once committed to a *SnapLock Compliance* Volume with retention controls, the standard file cannot be modified, appended to, or deleted until the expiration of the applied retention period.
  2. WORM-appendable file: Data may be appended to a WORM-appendable file, even after it has been committed with retention controls to a *SnapLock Compliance* Volume. After a segment is written, it cannot be modified or deleted until the retention expiration date is in the past.
     - The initial WORM-appendable file is committed to storage and retention controls, including *retention expiration date*, are applied.
     - New data appended to the end of the file is automatically committed to WORM in 256KB segments, with each new append segment automatically inheriting the retention controls, including *retention expiration date*, of the initial file.
     - In situations where the *final* append segment has less than 256KB of data, it is appended to the end of the file by either: (a) the source system explicitly changing the last segment to read-only or (b) the Autocommit process, if configured, identifying the last incomplete segment and setting it to read-only.
  3. Snapshots: The *SnapLock for SnapVault* archive process captures a snapshot of a Volume, according to the rules defined in a SnapMirror Policy. The snapshot is retained for the specified retention period and protected against modifications or overwrites for its lifespan.
- Critical metadata, retained for files and snapshots, includes:
  - **Files:** Unique file name, storage timestamp, unique Identifier, legal hold attribute (Y/N), atime[14] (retention expiration date), retention expiration date, and read-only attribute.
    - Only the legal hold (Y/N) and atime attributes may be modified for a record. Note: The atime attribute may only be extended, not shortened.
  - **Snapshots:** Unique Identifier (UUID), snapshot timestamp, expiry property (retention expiration date) and snapshot protection attribute.

[14] The atime is the last accessed attribute and when the atime is set to a future date, it is interpreted as a retention expiration date.

- Only the expiry property may be modified for the record. Note: The expiry property (retention expiration date) may only be extended, not shortened.

- For **snapshots**, *SnapLock Compliance* supports only time-based retention for compliance with the Rule:
  - A SnapMirror policy is defined, using the *SnapLock for SnapVault* feature, to (a) map a source Volume to a target *SnapLock Compliance* Volume, (b) set the snapshot type to ***snapshot protection***, and (c) provide a fixed retention duration.
    - According to the schedule defined within the policy, the snapshot is captured and an expiry date (retention expiration date) is computed by adding the policy's fixed retention duration to the current value of the Volume Compliance Clock. The calculated expiry period and a snapshot protection attribute (inherited from the *SnapLock Compliance* Volume) are assigned to the record and stored in a private metadata file within the *SnapLock Compliance* Volume.
    - Note: A maximum of 1,019 SnapMirrror snapshots may be saved in a SnapLock Compliance Volume, assuming sufficient storage space has been allocated to the Volume.
- For **files**, *SnapLock Compliance* supports both time-based and event-based retention options for committing a record in a manner that meets the requirements of the Rule:
  - **Time-Based Retention**, which specifies a fixed length of time to retain a file, is set using one of the following two methods:
    1. Both a *retention expiration date* and the *read-only* attribute are explicitly set in the inode when:
       - The source system transmits the record, via NFS, or SMB/CIFS protocols, with a *read-only* attribute and the *atime* attribute set to the *retention expiration date*.
       - The ONTAP CLI or REST APIs are used to set the *read-only* attribute and *retention expiration date* for a record.
       - The source system utilizes the API interface to set the record to *read-only* and set the *atime* value to the *retention expiration date***.** Optionally, the *atime* value can be set to Infinite. This special retention value indicates the record is to be retained permanently and may not be overridden or deleted by any user.
    2. Volume-level *SnapLock Compliance* default settings, when properly configured, automatically apply retention controls during the storage process. For example:
       - If the file is transmitted with a *read-only* attribute, but a retention expiration date is not transmitted, the Volume's Default Retention Period is used to calculate and store the retention expiration date.
       - If the *read-only* attribute is not transmitted for a file (with or without an explicit retention expiration date), after the wait period, Autocommit (if configured) sets the file to *read-only* and uses the Volume's Default Retention Period to calculate and store the retention expiration date. *Note: There are certain circumstances when the Minimum Retention Period is applied rather than the Default Retention Period. Care must be taken to assure the appropriate retention duration is applied.*

- **Event-Based Retention** policies, which may be applied to files and WORM-appendable files, are name-value pairs comprised of a policy name and retention duration, which is specified in terms of the number of days, weeks, months, or years to retain a record after the event occurs. Event-based retention policies are applied at the SVM level.
  - When utilizing event-based retention, Cohasset recommends the source system first transmit a *read-only* attribute and an explicit retention expiration date to establish baseline retention controls for the file. After the baseline retention controls are applied, the *atime* value may be changed to a special retention value of **Unspecified** (i.e., until the event occurs). This combination of actions preserves the explicitly-set retention period (i.e., the baseline *atime* value) and sets a special Unspecified flag on the inode, assuring immutable retention of the record continues (a) for the duration of the baseline retention period and (b) indefinitely thereafter, until the final retention expiration date is applied.
  - When the source system determines that an event has occurred, the appropriate event-based retention policy is applied at the Volume, directory, or record level. This applies the following controls:
    - The *read-only* attribute is automatically set (if not already set by the source system, as outlined in the preceding recommended process).
    - The Unspecified flag is automatically removed.
    - An explicit retention expiration date is calculated for the record by adding the retention duration defined for the event-based policy to the current Volume Compliance Clock value. This calculated date, if greater than the existing *atime* value, is applied as the new *atime* value for the record and stored in the inode of the file system.
  - If an attempt is made to apply event-based retention on a record under legal hold, the operation will fail.
  - Minimum and Maximum retention values established for the *SnapLock Compliance* Volume are not utilized when an event-based retention policy is applied.
  - Event-based policies can be applied multiple times to a single file; each time will result in an extension of the current *atime* value, which is also stored in the inode.
  - An event-based policy may define the retention duration as *Infinite* for records that must be retained permanently.
  - Values associated with an event-based retention policy may be changed at any time, which will have no effect on existing retention expiration dates already applied to records via that event-based retention policy.

- When time-based retention, event-based retention, or a legal hold is applied to a record stored in a *SnapLock Compliance* Volume (regardless of whether the record is stored on Primary Tier or Capacity Tier storage) integrated software controls are applied which ***prohibit*** the following actions, whether by the source system or administrative actions:
  - Deleting a record and its associated metadata prior to the retention expiration date.

- Decreasing (shortening) the retention expiration date for a record. A retention expiration date may be extended (lengthened) as necessary, unless a legal hold is currently applied (see Section 2.2.3.4, *Legal Holds (Temporary Holds)*, for more details).
- Altering or modifying stored record content, even after the retention period has expired.
- Moving a record to a new Volume.
- Renaming a record or renaming a directory, which could hide the file or access path.
- Utilizing *Privileged Delete*. This command is not allowed for *SnapLock Compliance* Volumes.

- A record (standard file or WORM-appendable file) may be **copied** to a new Volume (*SnapLock* or non-*SnapLock*). The copy (a) will be set to read-only, (b) the WORM flag will NOT be set in the inode and (c) the *atime* will be reset to current system time. If retention controls are required for the copy, it must first be converted to a read-write status, after which retention controls (e.g., read-only attribute and *atime* set to a future date) may be applied.
- *SnapLock Compliance* Volumes may not be **moved** to a different file system.

2.2.3.4 Legal Holds (Temporary Holds)

When litigation or a subpoena requires records to be placed on hold, which could entail retaining them beyond their assigned retention period, the regulated entity must ensure the subject records are protected for the duration of the legal hold. Holds are managed using the methods described in the following two subsections.

2.2.3.4.1 Files

- Legal hold functionality is supported for standard files and WORM-appendable files, stored in *SnapLock Compliance* Volumes that are properly configured for use with the *SnapLock* audit log. *SnapLock* audit log entries are automatically created when legal holds are applied or removed.
- Authorized users may place a legal hold on (a) the contents of one or more *SnapLock Compliance* Volumes, (b) records within a specified directory or folder, or (c) individual standard files and WORM-appendable files.
- Once a legal hold is applied:
  - Retention settings assigned to the affected records, if any, are suspended. Records subject to a legal hold are retained indefinitely and no modifications are allowed, including:
    - Extending the retention period associated with the records.
    - Applying an explicit retention expiration date to records that are under event-based retention.
  - If applied at the Volume level, a legal hold will apply to existing records; new records stored in the Volume moving forward will not automatically be protected by the legal hold.
  - All legal hold metadata (such as case name and/or ID), affected records, etc., are maintained separately in the tamper proof public inode space of the Volume.
- When a legal hold is no longer required, it may be removed. Once all legal holds have been removed for a given record, immutability controls are once again governed by the retention controls assigned to the record.

- There is no restriction on the number of records that can be included in a single legal hold. However, each record has a limit of 255 legal holds and each *SnapLock Compliance* Volume can support a maximum of 65,535 legal holds.

2.2.3.4.2 Snapshots

- When a legal hold requires retention of a snapshot beyond its assigned retention expiration date, the retention expiration date must be extended. Multiple extensions may be required to assure retention for the duration of the hold.

2.2.3.5 Deletion

- Records must meet the following conditions to be eligible for deletion:
  - The retention expiration date for the record must be in the past,
  - The Unspecified flag must be removed, and
  - Applied legal holds must be released.
- Eligible records can be deleted by the source system or authorized FSx for ONTAP users. As part of the deletion process, any replicas of the primary record are automatically removed.
- Modification of a record is not allowed over its lifespan, even after its retention period has expired and it is eligible for deletion.
- *SnapLock Compliance* Volumes may be deleted after all records retained in the Volume have passed their applied retention period.

2.2.3.6 Security

- Amazon FSx is designed to meet enterprise security and compliance requirements.
- Additionally, Amazon FSx supports the following types of controls:
  - Multiple levels of access control, including:
    - Amazon Virtual Private Cloud (VPC) security groups at the file system level.
    - AWS Identity and Access Management (IAM).
    - Unix permissions, NFS access control lists (ACLs) and New Technology File System (NTFS) ACLs at the file and folder levels.
    - Amazon FSx can be joined to an Active Directory to allow users to authenticate using their Active Directory credentials.
    - Multi-factor authentication (MFA).
  - Secure Sockets Layer (SSL)/Transport Layer Security (TLS) (1.2 or later) to communicate with AWS resources.
  - AWS server-side encryption, using AWS Key Management System (KMS) to prevent unauthorized access of the data.

2.2.3.7 Clock Management

FSx for ONTAP relies on the following types of secure Compliance Clocks to govern retention time:

- A *System Compliance Clock (SCC)* is maintained for each FSx for ONTAP file system. The SCC is synchronized with an Amazon Network Time Protocol (NTP) server at file system creation and regularly resynchronized to ensure current-time accuracy.
- A *Volume Compliance Clock (VCC)* is maintained for each *SnapLock Compliance* Volume. The VCC is initially synchronized with the SCC at Volume creation and regularly resynchronized to ensure current-time accuracy. The VCC is utilized to determine the retention expiration date for records stored within the Volume.

Once the SCC and VCC are initialized, clock values cannot be modified by any end users or system administrators. These controls prevent any inadvertent or intentional administrative modifications of the time clock, which could allow for premature deletion of records.

2.2.4 Additional Considerations

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

- Configuring any Volume that may be utilized to store SEC-regulated books and records with the *SnapLock* retention mode of *Compliance,* and assuring sufficient storage capacity is allocated.
- Ensuring both time-based and event-based retention controls are set for all required records, which includes properly configuring and understanding the applicability of the Default and Minimum retention periods, when the Autocommit feature is used.
- Managing event-based retention of files and WORM-appendable files by first setting an explicit baseline retention expiration date, then setting the Unspecified flag, to assure protection of records until the event occurs and an explicit retention period is applied.
- Monitoring for the successful application of event-based retention policies to ensure no conflicts occurred with a controlling legal hold and taking corrective action as necessary.
- Monitoring for the successful and appropriate application of legal holds to existing and new files and WORM-appendable files stored on *SnapLock Compliance* Volumes. Extending retention periods as necessary to meet legal hold preservation requirements for snapshots.
- Cohasset recommends setting the appropriate Default, Minimum and Maximum retention periods, as well as the Autocommit-wait period, for *SnapLock Compliance* Volumes, even if the source system intends to consistently send explicit retention controls. It is important to note that *SnapLock Compliance* always sets initial values for these parameters when a Volume is created. However, the regulated entity should modify the values, as appropriate, to meet the requirements of the Rule for stored records. Cohasset recommends Autocommit be set to 24 hours or less, to assure records are protected with *SnapLock Compliance* within 24 hours of storage. This recommendation is made to ensure that every record is protected with retention controls.

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 another compliant storage system, (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 FSx for ONTAP 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 FSx for ONTAP Capabilities

The recording and post-recording verification processes of FSx for ONTAP are described below.

2.3.3.1 Recording Process

- Amazon utilizes advanced electronic recording technology in its Primary Tier and Capacity Tier storage environments. Amazon's recording technology applies a combination of checks and balances to assure that the records are written in a high quality and accurate manner.
- ONTAP automatically calculates a checksum for every block of data transmitted for storage to ensure that all blocks are written in an accurate and complete manner. The checksums are retained for use in post-recording verification processes.
- Additionally, during the initial write process, the source system can request a hash digest 'fingerprint' (SHA 256 or MD5) be calculated by FSx for ONTAP and returned for its use, such as for verifying the integrity of requested records.
  - A hash digest 'fingerprint' cannot be generated for an entire snapshot however, it can be generated for individual files contained with the snapshot.
  - The source system may retain the hash digest for periodic post-recording validation processes.

2.3.3.2 Post-Recording Verification Process

- During retrieval of a record, FSx for ONTAP calculates a checksum for each block of data and compares it to the stored value to ensure that the data has not been altered or damaged in any way.
- Hash digest 'fingerprints' can be generated on-demand by ONTAP (i.e., at the request of the source system). The source system can compare the on-demand hash digest values to the original value (if retained by the source system) to assure continued integrity, during retrieval and periodically during the retention period.

2.3.4 Additional Considerations

- The source system is responsible for transmitting the complete contents of the required records, and Cohasset recommends utilizing HTTPS (a secure internet transfer protocol), when practical, to reduce the chance of network-level errors when transmitting the records.
- For retrieval, Cohasset recommends that the source system request a hash digest fingerprint be generated for the record, for validation of continued integrity.

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 either a:

- Human readable format that can be naturally read by an individual, or
- 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 Audit-Trail*.

2.4.2 Compliance Assessment

It is Cohasset's opinion that the functionality of FSx for ONTAP meets this SEC requirement to maintain the capacity to readily download and transfer the records and information in FSx for ONTAP used to locate the records when the considerations described in Section 2.4.4 are satisfied.

2.4.3 FSx for ONTAP Capabilities

The following capabilities relate to the requirement for capacity to download and transfer the records and the information needed to locate the records.

2.4.3.1 Files

- ONTAP utilizes the inode to uniquely identify records stored within a *SnapLock Compliance* Volume. The inode contains record metadata and points to the specific blocks of data that make up the record content, regardless of whether it is stored on Primary Tier or Capacity Tier storage.
  - ONTAP stores the file name submitted by the source system which then allows the source system to request one or more specific records to be downloaded for viewing, reproduction, or transfer to a medium acceptable under the Rule.

- The directory of a *SnapLock Compliance* Volume, including file name, date stored and other directory attributes (metadata) can be viewed by the source system or an authorized administrator. The appropriate records can then be identified, retrieved and downloaded, whereupon they can be transferred using local capabilities to any medium acceptable under the Rule.

2.4.3.2 Snapshots

- ONTAP stores metadata associated with snapshots in private metadata files within the *SnapLock Compliance* Volume.
  - Lists of snapshots stored within each Volume, including attributes such as UUID, expiry date, and storage timestamp can be produced via CLI commands or programmatically via APIs.
  - Snapshots may be restored to a specified source location where content may then be viewed, reproduced or transferred to a medium acceptable under the Rule.

2.4.4 Additional Considerations

For this requirement, the regulated entity is also 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 FSx for ONTAP 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.[15] [emphasis added]

[15] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66421.

- 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.[16] [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 FSx for ONTAP 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 as described in Section 2.5.3 and (b) the considerations described in Section 2.5.4 are satisfied.

2.5.3 FSx for ONTAP Capabilities

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

2.5.3.1 Redundant Set of Records

For compliance with paragraph (A), to maintain a redundant set of records, FSx for ONTAP must be configured in one of the following deployment types:

- **Single-AZ**: With this type of deployment, Amazon FSx automatically provisions a pair of file servers in an active-standby configuration. Primary and secondary file servers are in separate fault domains, within a single Availability Zone. Amazon FSx automatically replicates data to the secondary file servers to protect against component failures or data corruption, and to provide continuous access during file system maintenance periods. In the event of a component failure or unexpected service disruption, Amazon FSx immediately fails over to the standby file server with no manual intervention required.
- **Multi-AZ**: In addition to the availability and durability features of the Single-AZ deployment, the Multi-AZ deployment protects against disruptions within a single Availability Zone. The secondary server is deployed in a different Availability Zone than the primary and data is kept synchronized across the Availability Zones.

2.5.3.2 Other Redundancy Capabilities

For compliance with paragraph (B), FSx for ONTAP redundantly stores data blocks of records across multiple disks. In the event of data corruption or disk failure, the original record can be regenerated from the data stored on other disks. The redundantly stored data blocks are retained for the full retention period and any applied legal holds.

2.5.4 Additional Considerations

In addition, for this requirement, the regulated entity is responsible for: (a) maintaining its account in good standing, (b) properly configuring the FSx for ONTAP file system as either a Single or Multi-AZ deployment type

[16] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66421.

for compliance with paragraph (A) of this requirement, (c) maintaining volume storage capacity, encryption keys, and other information and services needed to use FSx for ONTAP and permit access to the redundant records.

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 FSx for ONTAP supports the regulated entity's efforts to meet this SEC audit system requirement.

2.6.3 FSx for ONTAP Capabilities

The regulated entity is responsible for an audit system and compliance is supported by FSx for ONTAP.

- When inputting files, the source system must transmit a unique name identifier with every file. Additionally, FSx for ONTAP stores a unique identifier and system-generated recording timestamp for each file. These attributes are immutable, chronologically account for each inputted file and are retained for the same time period as the record.
- When inputting snapshots, FSx for ONTAP assigns a Unique Identifier (UUID) to each snapshot and stores a system-generated recording timestamp. These attributes are immutable, chronologically account for each inputted snapshot, and are retained for the same time period as the record.
- Standard files, each stored segment of a WORM-appendable file, and snapshots are immutably stored over their lifespan; therefore, no changes are allowed once the file or snapshot is stored.
- In addition to the immutable record metadata, the *SnapLock* audit log captures lifecycle events for records, such as:
  - Adding records to a *SnapLock Compliance* Volume,
  - Setting initial retention for a record, including event-based retention,

- Extending the retention expiration date for a record,
- Applying and removing legal holds,
- Deleting eligible records that are past their retention expiration date.

- *SnapLock* audit logs are retained in a separate *SnapLock* Audit Log Volume, which can be configured in *Compliance* or *Enterprise* mode. A default retention period of six months is set for the Audit Log Volume and cannot be shortened, only extended if necessary. The regulated entity may export selected audit events to a security information and event management tool for retention.

2.6.4 Additional Considerations

The regulated entity is responsible for maintaining an audit system for inputting records and may utilize FSx for ONTAP features alone or in conjunction with another system.

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

This section contains a summary assessment of the functionality of FSx for ONTAP, as described in Section 1.3, *FSx for ONTAP 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 audit-trail and (2) non-rewriteable, non-erasable, 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.*[17] [emphasis added]

Cohasset's assessment, in Section 2, pertains to FSx for ONTAP, with *SnapLock Compliance*, which is a highly restrictive configuration that assures the storage solution applies integrated controls to (a) protect immutability of the record content and certain system metadata and (b) prevent deletion over the applied retention period.

In the following table, Cohasset correlates the functionality of FSx for ONTAP, using *SnapLock Compliance*, with the *principles-based* CFTC requirements related to the *form and manner of retention* and the *inspection and production of regulatory records*. In addition, Cohasset contends that FSx for ONTAP, using the less restrictive *SnapLock Enterprise,* meets these *principles-based* CFTC requirements, when the regulated entity applies appropriate procedural controls to oversee operations that may allow content to be modified or deleted prior to expiration of the retention period. This less restrictive *SnapLock Enterprise mode* provides flexibility for authorized users to delete WORM files before their retention period expires, which may be beneficial for compliance with privacy and data protection requirements. The first column enumerates the CFTC regulation. The second column provides Cohasset's analysis and opinion regarding the ability of FSx for ONTAP to meet the requirements for electronic regulatory records in CFTC Rule 1.31(c)-(d).

[17] 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[18] with time-based and event-based retention periods, are met by the functionality of FSx for ONTAP, with either *SnapLock Compliance or Enterprise mode*. This report describes the functionality of FSx for ONTAP, with *SnapLock Compliance,* 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] FSx for ONTAP retains immutable metadata attributes, e.g., unique ID and filename, as an integral component of the records, and, therefore, these attributes are subject to the same retention protections 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. Further, FSx for ONTAP in conjunction with the *SnapLock* audit log captures lifecycle events for records and provides storage options to extend the default six-month retention period set for the Audit Log Volume. For additional information, see Section 2.6, *Audit System*.
(ii) Systems that ensure the records entity is able to produce electronic regulatory records in accordance with this section, and ensure the availability of such regulatory records in the event of an emergency or other disruption of the records entity's electronic record retention systems; and	It is Cohasset's opinion that FSx for ONTAP capabilities described in Section 2.5, *Record Redundancy*, including methods for a persistent duplicate copy or 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).

[18] If FSx for ONTAP retains the regulatory record content and core metadata attributes but does not necessarily retain other information needed to satisfy this definition of a regulatory record (such as information to augment search and data on how and when the records were created, formatted, or modified), the regulated entity is responsible for retaining and managing this other information in a compliant manner.

CFTC 1.31(c)-(d) Regulation [emphasis added]	**Compliance Assessment Relative to CFTC 1.31(c)-(d)**
(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 FSx for ONTAP 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 FSx for ONTAP[19] 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 FSx for ONTAP, when properly configured, has the following functionality, which meets the regulatory requirements:

- Retains the records and immutable system metadata in non-rewriteable, non-erasable format for time-based retention periods by applying *SnapLock Compliance* controls. Additionally, provides the ability to apply event-based retention controls to standard files and WORM-appendable files.
- Applies legal holds to preserve records (i.e., standard files and WORM-appendable files stored in *SnapLock Compliance* Volumes) for a subpoena, legal hold or similar circumstances.
- Prohibits deletion of records until the retention expiration date has expired and any applied legal hold has been removed.
- Verifies the accuracy of storing and retaining the records, using checksums and FSx for ONTAP validation processes.
- Provides capacity for authorized users to readily access the Volume using local tools to (a) find and download records and information needed to locate the records, (b) render a human readable view and (c) produce a reasonably usable electronic format.
- Maintains records redundancy to retrieve an accurate replica of the record from a persistent duplicate copy, or reestablish the record from an alternate source, should an error occur in one segment of the data 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 FSx for ONTAP, 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).

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

5 • 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.

5.1 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[20] 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.*[21] [emphasis added]

These 2022 amendments (a) provide a record 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.*[22] [emphasis added]

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

5.1.1 Record Audit-Trail Alternative

The objective of the record audit-trail requirement is to allow regulated entities to keep required records on business-purpose recordkeeping systems.

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

[21] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66428.

[22] 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.*[23] [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.*[24] [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."*[25] [emphasis added]

5.1.2 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****[26] [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).

---

23 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.
24 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.
25 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66418.
26 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.*[27] [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.*[28] [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.*[29] [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 FSx for ONTAP related to each requirement.

5.2 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).[30]

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.*

---

27 2003 Interpretative Release, 68 FR 25282.

28 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).

29 2003 Interpretative Release, 68 FR 25283.

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

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

Effective August 28, 2017, the Commodity Futures Trading Commission (CFTC) amended 17 CFR § 1.31 (CFTC Rule) to 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.*[31] [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 FSx for ONTAP in relation to each requirement, see Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*.

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

6 • Cloud Provider Undertaking

6.1 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 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 can (a) independently access the records, (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.[32] [emphasis added]

6.2 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 on FSx for ONTAP, 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.

6.3 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) maintaining technology, resource capacity, encryption keys and privileges to access FSx for ONTAP, and (e) 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.

[32] 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.