

VAST DataStore

COMPLIANCE ASSESSMENT

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

Abstract

The VAST DataStore consolidates file and object storage on a single data platform with all-flash performance and cloud scalability. VAST Views are protocol-independent, virtual containers with features to enable retention controls applied to records in compliance with SEC electronic recordkeeping requirements. Additionally, retention controls can be set on snapshots, which are virtual point-in-time archive copies of any directory.

In this report, Cohasset Associates, Inc. (Cohasset) assesses the functionality of the VAST DataStore (see Section 1.3, *VAST DataStore 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 the VAST DataStore, when properly configured and used with *File Retention* or *S3 Retention 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 the VAST DataStore 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.

Table of Contents

Abstract	1
Table of Contents	2
1 • Introduction	3
1.1 Overview of the Regulatory Requirements	3
1.2 Purpose and Approach	4
1.3 VAST DataStore Overview and Assessment Scope	5
2 • Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e)	7
2.1 Record and Audit-Trail	7
2.2 Non-Rewriteable, Non-Erasable Record Format	8
2.3 Record Storage Verification	25
2.4 Capacity to Download and Transfer Records and Location Information	26
2.5 Record Redundancy	28
2.6 Audit System	30
3 • Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)	32
4 • Conclusions	35
Appendix A • Overview of Relevant Electronic Records Requirements	36
A.1 Overview of SEC Rules 17a-4(f) and 18a-6(e) <i>Electronic Recordkeeping System</i> Requirements	36
A.2 Overview of FINRA Rule 4511(c) <i>Electronic Recordkeeping System</i> Requirements	38
A.3 Overview of CFTC Rule 1.31(c)-(d) <i>Electronic Regulatory Records</i> Requirements	39
About Cohasset Associates, Inc.	40

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 the VAST DataStore 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 entities¹, the SEC stipulates recordkeeping requirements, including retention periods.

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

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

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

1.1.2 FINRA Rule 4511(c) Requirements

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

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

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

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

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

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

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

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

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

1.2 Purpose and Approach

To obtain an independent and objective assessment of the compliance capabilities of the VAST DataStore for preserving required electronic records, VAST Data 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.

VAST Data engaged Cohasset to:

- Assess the functionality of the VAST DataStore, 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 the VAST DataStore; 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 the VAST DataStore and its functionality or other VAST Data products or services. The information utilized by Cohasset to conduct this assessment consisted of: (a) oral discussions, (b) product demonstrations, including system setup and configuration, (c) system documentation, (d) user and system administrator guides, and (e) related materials provided by VAST Data 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 VAST DataStore Overview and Assessment Scope

1.3.1 VAST DataStore Overview

The VAST DataStore consolidates file and object storage on a single data platform with all-flash performance and cloud scalability. VAST Views are protocol-independent, virtual containers with features to enable retention controls applied to records⁴ in compliance with SEC electronic recordkeeping requirements. Additionally, retention controls can be set on snapshots, which are virtual point-in-time archive copies of any directory.

The **VAST DataStore** is the storage foundation and is responsible for persisting data and making it available via various storage protocols. The VAST DataStore architecture is depicted in the following Figure:

- ▶ The **Protocol Layer** supports and is compatible with multiple storage protocols, including:
 - Network File System (NFS) and Server Message Block (SMB) file storage protocols.
 - Simple Storage Service (S3) object protocol.
- ▶ The **VAST Management System** (VMS) provides a graphical user interface (GUI), command line interface (CLI) and REST application protocol interface (VMS API).
- ▶ The **Element Store** is an abstraction layer designed to facilitate storage flexibility and interoperability. Relevant to this report, the Element Store contains:
 - **VAST Metadata**, which is a built-in 'share everything' metadata repository and includes, but is not limited to, file and object metadata, tree structure, NFS v4.1 extended attributes, S3 tags, and retention and legal hold statuses. Selected VAST Metadata is made accessible in the **VAST Catalog**, which can be queried using simple SQL queries.
 - Deduplicated unique data, which is represented in Figure 1 as a parent-child hierarchy with files and objects, as well as snapshots.
- ▶ **VAST Views** are protocol-independent, virtual containers of the assigned storage path. A VAST View is configured to enable access by NFS, SMB and S3 storage protocols. For compliance with the non-rewriteable,

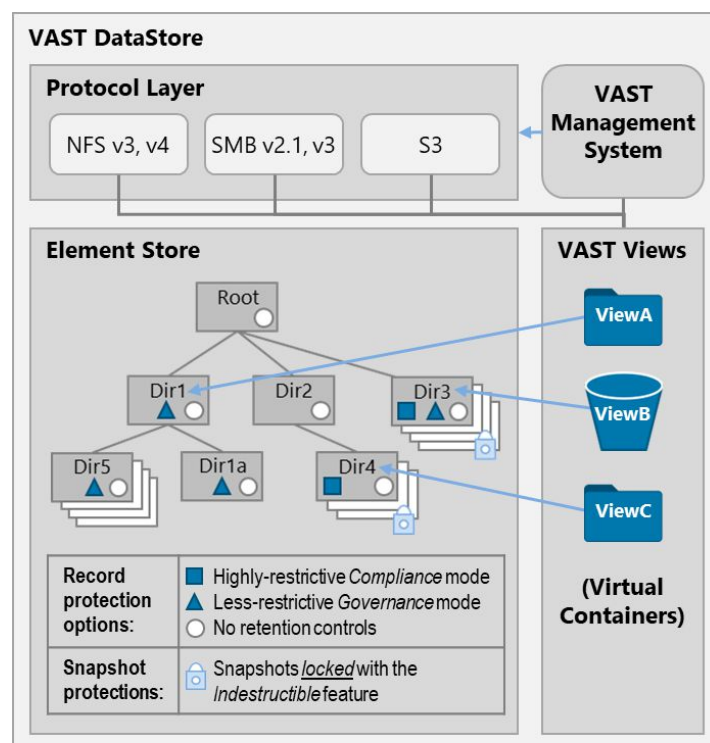


Figure 1: VAST DataStore high-level architecture

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

non-erasable requirement of the Rules, the *WORM-enabled* feature must be enabled on a View (hereinafter a *WORM-enabled View*).

- A *WORM-enabled View* must be configured with either *File Retention* or *S3 Retention* features. When records are stored in the directory (i.e., storage path) of a *WORM-enabled View*, retention controls may be applied and set to (a) highly-restrictive *Compliance* mode or (b) less-restrictive *Governance* mode. In this report, Cohasset assesses the highly-restrictive *Compliance* mode. See Section 2.2.3.3, *Records and Retention Controls*, for details.
 - A *WORM-enabled View* cannot contain nested Views under it and is restricted to either file or S3 storage protocols. See Section 2.2.3.2, *View Capabilities and View Retention Configurations*, for details.
 - Additionally, a second View cannot be set for the same storage path as a *WORM-enabled View*.
- A **Snapshot** is a virtual point-in-time archive copy of any directory, whether or not the directory is configured as a View.
- Snapshots are created by Protection Policies, which calculate a *Snapshot Expiry Timestamp* by adding the retention period stipulated in the Protection Policy to the snapshot creation date. The *Snapshot Expiry Timestamp* is stored as metadata of the snapshot.

The retention controls applied to the Protection Policies and snapshots are considered locked and cannot be changed and deletion is prohibited until the *Snapshot Expiry Timestamp* is in the past, when *Indestructibility* features are applied and enforced. However, the *Indestructibility* feature can be suspended by authorized administrators that obtain a time-limited token from VAST Data support personnel. When the *Indestructibility* feature suspended, the Protection Policies and snapshots are unlocked, which allows changes to retention configurations and deletion before the *Snapshot Expiry Timestamp*. *Therefore, procedural controls and monitoring are required to scrutinize actions taken to shorten or remove retention controls and prematurely delete required snapshots.*

1.3.2 Assessment Scope

The scope of this assessment is focused specifically on the compliance-related features of the VAST DataStore, including but not limited to, (a) *WORM-enabled Views* configured with *File Retention* or *S3 Retention*, when highly-restrictive *Compliance* mode is applied to each required record, and (b) snapshots when *Indestructibility* features are applied, enforced and locked, which enforce less-restrictive retention controls.

This report assesses the VAST DataStore, release 4.7 GA, when properly configured and deployed on-premises, using hardware qualified by VAST Data.

NOTE: This reports excludes:

- Protocols, other than those specifically listed as included.
- Tables and stored elements other than files and objects.
- Software as a Service (SaaS) and Platform as a Service (PaaS) solutions using the VAST DataStore, when a third party manages or provides the solution to the regulated entity.

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

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

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

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

2.1 Record and Audit-Trail

2.1.1 Compliance Requirement

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

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

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

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

- (1) All modifications to and deletions of the record or any part thereof;
- (2) The date and time of actions that create, modify, or delete the record;
- (3) If applicable, the identity of the individual creating, modifying, or deleting the record; and
- (4) Any other information needed to maintain an audit-trail of the record in a way that maintains security, signatures, and data to ensure the authenticity and reliability of the record and will permit re-creation of the original record if it is modified or deleted

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

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

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

[T]he audit-trail requirement applies to the final records required pursuant to the rules, rather than to drafts or iterations of records that would not otherwise be required to be maintained and preserved under Rules 17a-3 and 17a-4 or Rules 18a-5 and 18a-6.⁶ [emphasis added]

2.1.2 Compliance Assessment

In this report, Cohasset has not assessed the VAST DataStore 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 the VAST DataStore, with the features and controls described in Sections 2.2 through 2.6 of this report.

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

2.2 Non-Rewriteable, Non-Erasable Record Format

2.2.1 Compliance Requirement

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

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

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

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

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

a process of integrated software and hardware codes and clarified that “a software solution that prevents the overwriting, erasing, or otherwise altering of a record during its required retention period would meet the requirements of the rule.”

In 2001, the Commission issued guidance that Rule 17a-4(f) was consistent with the ESIGN Act. The final amendments to Rule 17a-4(f) do not alter the rule in a way that would change this guidance.⁷ [emphasis added]

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

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

2.2.2 Compliance Assessment

It is Cohasset’s opinion that the functionality of the VAST DataStore, with *File Retention* or *S3 Retention* applied in *Compliance* mode, meets this SEC requirement to retain records in non-rewriteable, non-erasable format for the applied time-based⁹ 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.

Additionally, by setting the *Indestructible* option, less-restrictive retention controls may be applied to snapshots, which are point-in-time archive copies of a directory. Note: These retention controls are considered to be less-restrictive, since the *Indestructibility* features may be suspended, using a time-limited token provided by VAST Data support personnel. When the *Indestructibility* feature is suspended, the Protection Policies and snapshots are unlocked, which allows changes to retention configurations and premature deletion. *Therefore, procedural controls and monitoring are required to scrutinize actions taken to shorten or remove retention controls and prematurely delete snapshots.*

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

2.2.3 VAST DataStore Capabilities

This section describes the functionality of the VAST DataStore 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.

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.

2.2.3.1 Overview

- ▶ As a multi-protocol solution, VAST Data offers both *File Retention* and *S3 Retention* features, which are designed to meet this SEC requirement for non-rewriteable, non-erasable record format. Specifically, *Compliance* mode applies highly-restrictive integrated control codes and is the subject of this Compliance Assessment Report.
 - To apply time-based retention controls to records, the View must be properly configured and either (a) the source system must transmit explicit retention attributes (e.g., for files, an *Atime* value with a future date and a *Read-Only* attribute; for objects, a *Retain Until Date* and *Compliance* retention mode) to apply to the record or (b) the View must be configured to automatically apply appropriate *Default Retention* values to stored records. See Section 2.2.3.3, *Records and Retention Controls*, for additional details.
- ▶ Additionally, retention configurations on Protection Policies and retention controls on snapshots, which are point-in-time archive copies of a directory, can be set to *Indestructible*. When *Indestructibility* features are applied and enforced, retention settings cannot be changed and deletion is prohibited until the *Snapshot Expiry Timestamp* is in the past.
 - However, one or two authorized administrators may obtain a time-limited *token* issued by VAST Data support personnel, to suspend the *Indestructibility* features, which unlocks the Protection Policies and snapshots, allowing retention configurations to be changed and snapshots to be deleted before the *Snapshot Expiry Timestamp*.
- ▶ The following table summarizes the retention controls applied to records by *File Retention* and *S3 Retention*, in *Compliance* mode, and snapshots when *Indestructibility* features are applied, enforced and locked. See the subsections following this *Overview*, for information on configuring the retention features and the resulting integrated controls.

	<i>File Retention</i> or <i>S3 Retention</i> , in <i>Compliance</i> mode	Snapshots, with <u>locked</u> <i>Indestructibility</i> features
Protecting record content	• With <i>File Retention</i>, write permissions are disabled for the lifespan of the record, which protects the record content from modification or overwrite until record deletion. • With <i>S3 Retention</i>, versioning protects the record content for its lifespan. Any attempt to modify or overwrite results in storing a new version, with separate retention controls.	• Snapshots are designated as read-only, and therefore, are protected from modification or overwrite for its lifespan, until snapshot deletion.
Protecting immutable metadata	• Renaming a parent or child directory is <u>prohibited</u>. • With <i>File Retention</i>, changing a file name or an NFS alias or SMB share name is <u>prohibited</u>. • With <i>S3 Retention</i>, changing an object name, version identifier or S3 bucket name is <u>prohibited</u>.	• Snapshots are inextricably linked to the source directory and <u>cannot</u> be renamed.
Modifying retention controls	• Retention controls <u>cannot</u> be removed and <u>cannot</u> be downgraded to <i>Governance</i> mode. ◦ Accordingly, <i>Compliance</i> mode assures retention controls are <u>not</u> circumvented by any user or process.	• Protection Policies and snapshots <u>cannot</u> be deleted and retention controls <u>cannot</u> be changed, when <i>Indestructibility</i> features are applied, <u>enforced</u>, and <u>locked</u>.
Extending retention	• A record's <i>Retain Until Date</i> may be extended at any time.	• The <i>Snapshot Expiry Timestamp</i> applied to local and remote snapshots <u>can</u> be extended at any time.

	<i>File Retention or S3 Retention, in Compliance mode</i>	Snapshots, with <u>locked</u> Indestructibility features
Shortening retention	The record's <i>Retain Until Date</i> cannot be shortened. <i>Note:</i> For <i>File Retention</i>, when the <i>auto-commit</i> feature is configured, retention controls may be changed or removed during the <i>auto-commit</i> grace period.	- The <i>Snapshot Expiry Timestamp</i> applied to local and remote snapshots cannot be shortened, when the snapshot is <i>Indestructibility</i> features are applied, <u>enforced</u>, and <u>locked</u>. <i>Note:</i> When <i>Indestructibility</i> features are <u>suspended</u>, <i>Snapshot Expiry Timestamp</i> can be shortened and other retention controls can be changed; see Section 2.2.3.6, <i>Snapshot Configurations, Retention Controls and Deletion</i>.
Applying a legal hold	The record's <i>Legal Hold</i> attribute may be set (Yes) at any time and may be applied to any record in the storage path of a <i>WORM-enabled</i> View, whether or not the record has retention controls.	- Legal hold features are <u>not</u> available for snapshots. - See the row entitled Extending retention; preservation for legal holds may be met by extending the <i>Snapshot Expiry Timestamp</i>.
Preventing deletion	- Deletion of the <i>WORM-enabled</i> View is <u>prohibited</u>, unless the View is empty. - Deletion of directories in the storage path of a <i>WORM-enabled</i> View is <u>prohibited</u> unless the directory is empty. - Deletion of each record and its associated immutable metadata is <u>prohibited</u> until the applied <i>Retain Until Date</i> expires and the legal hold is clear (No). - When set to <i>Compliance</i> mode, the retention controls <u>cannot</u> be removed or circumvented by any user or administrator. - For <i>S3 Retention</i>, deletion of the record (without identifying the Version) appends a Delete Marker, which may be removed to reinstate the original record.	- When <i>Indestructibility</i> features are applied, <u>enforced</u>, and <u>locked</u>: - Deletion of the Protection Policy is <u>prohibited</u>. - Deletion of a snapshot is <u>prohibited</u> until its <i>Snapshot Expiry Timestamp</i> is in the past. <i>Note:</i> When the <i>Indestructibility</i> feature is <u>suspended</u>, the Protection Policies and snapshots are <u>unlocked</u>, which allows changes to retention configurations and premature deletion of snapshots; see Section 2.2.3.6, <i>Snapshot Configurations, Retention Controls and Deletion</i>.

2.2.3.2 View Capabilities and View Retention Configurations

- ▶ A View must be configured with a specific storage path. Further, for compliance with the Rules, the *WORM-enabled* feature must be enabled on a View (hereinafter a *WORM-enabled* View), and the View must be configured to support either *File Retention* (■) or *S3 Retention* (🗑️), as depicted in the following Figure.

- A *WORM-enabled* View cannot contain any nested Views under it and is restricted to either file or S3 storage protocols.
- A second View cannot be configured with the same storage path, if one of the Views is *WORM-enabled*.

- ▶ In Figure 2, records (files and object versions) are represented as stored in directories, though this hierarchy is virtual.

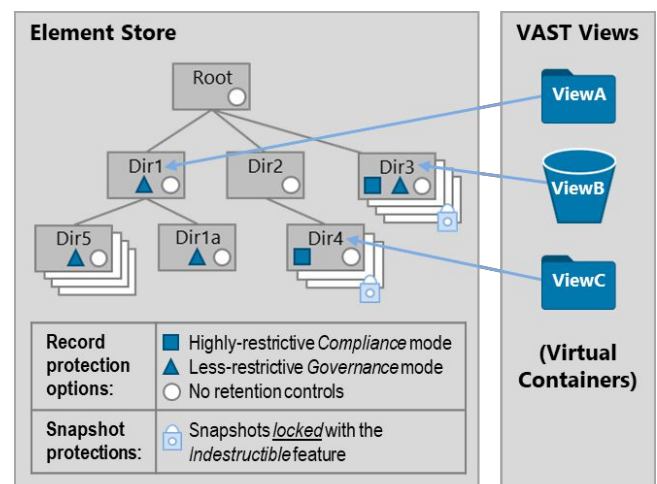


Figure 2: VAST DataStore high-level storage architecture

- When records (files or object versions) are in a directory associated with a *WORM-enabled View*, each record has separate retention controls applied to it, which may be: (a) highly-restrictive *Compliance* mode (■), (c) less-restrictive *Governance* mode (▲), or (c) no retention controls. In this report, Cohasset assesses the highly-restrictive *Compliance* mode. See Section 2.2.3.3, *Records and Retention Controls*, for details.
- Three Views are illustrated in Figure 2, which highlights the relationships between Views, directories (storage paths), and records.
- ViewA is configured for (a) storage path Dir1 and its children, Dir1a and Dir5, and (b) *File Retention* with NFS and/or SMB storage protocols and less-restrictive *Governance* mode.
 - ViewB is configured for (a) storage path Dir3 and (b) *S3 Retention* with the S3 protocol.
 - ViewC is configured for (a) storage path Dir4 and (b) *File Retention* with NFS and/or SMB storage protocols and highly-restrictive *Compliance* mode.
- **Snapshots** are illustrated as white icons behind directories. Snapshots apply to a directory and are independent of Views. **Protection Policies** create snapshots, which are read-only and serve as virtual point-in-time archive copies of the directory the policy protects. Snapshots may be taken of any directory (whether or not it is configured as a View). Also see Section 2.2.3.6, *Snapshot Configurations, Retention Controls and Deletion*.
- The following table describes the retention-related configurations for a *WORM-enabled View* setup for (1) *File Retention* with NFS and/or SMB storage protocols or (2) *S3 Retention* with the S3 protocol.

	1. <i>File Retention</i> Features (<i>WORM-enabled Views</i> configured for NFS and/or SMB storage protocols)	2. <i>S3 Retention</i> Features (<i>WORM-enabled Views</i> configured for the S3 protocol)
WORM-enabled	• The <i>WORM-enabled</i> feature <u>must</u> be enabled (i.e., a <i>WORM-enabled View</i>).	
Path	• The View <u>must</u> be assigned to a path (i.e., the parent level directory, which automatically includes any associated child directories).	
Protocols and data storage endpoints	• The protocols supported by the View <u>must</u> be selected, and the data storage endpoint is assigned a name: ○ When the NFS protocol is selected, the NFS alias is <u>optional</u>. ○ When the SMB protocol is selected, the SMB share name <u>must</u> be specified.	• When the S3 protocol is selected for the View, the S3 bucket name <u>must</u> be specified, as the data storage endpoint name.
Versioning	• Not applicable, since <i>File Retention</i> uses NFS and SMB protocols, which do <u>not</u> support the concept of versioned files.	• Versioning is automatically <u>enabled</u> (On) and <u>cannot</u> be turned off.
Retention Mode	• <i>File Retention Mode</i> is a <u>mandatory</u> configuration and may be set to either highly-restrictive <i>Compliance</i> mode or less-restrictive <i>Governance</i> mode. <u>Note</u>: This report assesses records set to <i>Compliance</i> mode; see Section 2.2.3.3.1, <i>Applying File Retention Controls</i>, for additional information. • The currently configured <i>File Retention Mode</i> for the View <u>automatically applies</u> to new records stored in the View with retention controls. The <i>File Retention Mode</i> is retained as metadata at the record-level.	• The <i>S3 Retention Mode</i> is an <u>optional</u> configuration. • When configured, it serves as a <u>Default</u> <i>S3 Retention Mode</i> and may be set to either highly-restrictive <i>Compliance</i> mode or less-restrictive <i>Governance</i> mode. <u>Note</u>: This report assesses record versions set to <i>Compliance</i> mode; see Section 2.2.3.3.2, <i>Applying S3 Retention Controls</i>, for additional information.

	1. File Retention Features (WORM-enabled Views configured for NFS and/or SMB storage protocols)	2. S3 Retention Features (WORM-enabled Views configured for the S3 protocol)
	- The <i>File Retention Mode</i> assigned to the View <u>can</u> be changed at any time, because it only applies to new records and does <u>not</u> retroactively impact previously stored records. - The <i>File Retention Mode</i> assigned to the View <u>cannot</u> be removed by any user.	- This <u>Default</u> S3 Retention Mode is <u>only</u> applied when the record version is transmitted <u>without</u> retention controls. - Since defaults only apply to records stored in the future and do <u>not</u> affect previously stored records, authorized users may change or remove the default configuration at any time. Note: If this <u>Default</u> S3 Retention Mode is set, the <u>Default Retention Period</u> must also be set, because these two configurations are a <u>pair</u>.
Default Retention Period	- The <i>Default Retention Period</i> (specified in terms of minutes, hours, days, or years) is an <u>optional</u> configuration. If set, it must honor the optional Min/Max boundaries. (See next row for <i>Min/Max retention periods</i>.) - When the default is configured and records are transmitted <u>without</u> retention controls, the <i>Default Retention Period</i> is added to the record's last modified timestamp to calculate and store its <i>Retain Until Date</i>. Accordingly, setting a <i>Default Retention Period</i> (together with the <i>File Retention Mode</i>) assures all records in the View are assigned retention controls. - The <i>Default Retention Period</i> assigned to the View <u>can</u> be changed or removed at any time, because it only applies to new records and does <u>not</u> retroactively impact previously stored records. Note: A <i>Default Retention Period</i> is <u>required</u> if either the <i>Min/Max Retention Periods</i> or the <i>auto-commit</i> feature are configured.	- The <i>Default Retention Period</i> (specified in terms of minutes, hours, days, or years) is an <u>optional</u> configuration. - When the default is configured and record versions are transmitted <u>without</u> retention controls, the <i>Default Retention Period</i> is added to the record version's last modified timestamp to calculate and store its <i>Retain Until Date</i>. Accordingly, setting a <i>Default Retention Period</i> (together with a <u>Default</u> S3 Retention Mode) assures all record versions in the View are assigned retention controls. - Since defaults only apply to records stored in the future and do <u>not</u> affect previously stored records, authorized users may change or remove the default configuration at any time. Note: If this <i>Default Retention Period</i> is set, the <u>Default</u> S3 Retention Mode must also be set, because these two configurations are a <u>pair</u>.
Min/Max Retention Periods	- The <i>Minimum and Maximum Retention Periods</i> (specified in terms of minutes, hours, days, or years) are <u>optional</u> and are set as a pair. - The <i>Min/Max Retention Periods</i> define boundaries to validate an explicit <i>Retain Until Date</i> that is transmitted with a record. - When the <i>Min/Max</i> is configured and a record is transmitted with an explicit <i>Retain Until Date</i> that is either too short or too long, the <i>Minimum</i> or <i>Maximum Retention Period</i> (respectively) is added to the record's last modified timestamp to calculate its <i>Retain Until Date</i>. Note: Setting the <i>Min/Max</i> requires a <i>Default Retention Period</i> to be configured.	Feature is <u>not available</u> for WORM-enabled Views configured for the S3 Retention features.
Auto-commit	The <i>auto-commit period</i> (specified in terms of minutes, hours, or days) is <u>optional</u> and requires a <i>Default Retention Period</i> to be configured. Allowable range is between 5 minutes and 30 days.	Feature is <u>not available</u> for WORM-enabled Views configured for S3 Retention features.

	1. File Retention Features (<i>WORM-enabled Views</i> configured for NFS and/or SMB storage protocols)	2. S3 Retention Features (<i>WORM-enabled Views</i> configured for the S3 protocol)
	- Duration of time that must lapse (grace period) from the record's last modified timestamp, after which the VAST DataStore applies retention controls to the record. During this grace period, the record is <u>not</u> retention protected and the record's retention controls may be removed or changed. <u>Note</u>: Setting the <i>auto-commit period</i> requires a <i>Default Retention Period</i> to be configured.	

2.2.3.3 Records and Retention Controls

- ▶ The following two subsections separately describe the methods of applying retention controls to records and record versions associated with *WORM-enabled Views*:
 - Section 2.2.3.3.1, *Applying File Retention Controls*, and
 - Section 2.2.3.3.2, *Applying S3 Retention Controls*.
- ▶ Additionally, Section 2.2.3.3.3, *Record Operations and Retention Controls*, compares the retention controls derived from *File Retention* and *S3 Retention*, when in *Compliance* mode.
- ▶ These retention features apply to records accessible through *WORM-enabled Views*. For retention features that apply to snapshots, see 2.2.4.6, *Snapshot Configurations, Retention Controls and Deletion*.

2.2.3.3.1 Applying File Retention Controls

- ▶ For *WORM-enabled Views* configured with *File Retention* and the NFS and/or SMB protocols, a record is an individual file with a unique file name within the directory where it is stored. Currently, the concept of versioning is not applicable to file storage protocols; therefore, versions are not supported by *File Retention* features.
 - After the retention controls are applied to a record, its contents are retained immutably over its lifespan.
 - Record metadata includes:
 - ◆ Immutable (unchangeable) metadata: Tenant, full path and file name, extended attributes in NFS v4.1, and creation (storage) timestamp, as well as *Compliance* mode and last modified timestamp after retention controls are applied.
 - ◆ Mutable (changeable) metadata: *Retain until date* (which can be extended, but not shortened), legal hold status, and other attributes in VAST 'Share-Everything' Metadata Store.
- ▶ For *WORM-enabled Views* configured with *File Retention* and the NFS and/or SMB protocols, two retention controls protect each record:
 1. *File Retention Mode*, which is applied to each record with retention controls. Once set to *Compliance*, the mode cannot be changed to *Governance* and cannot be removed. Also, see Section 2.2.3.2, *View Capabilities and View Retention Configurations*.

2. *Retain Until Date*, which is stored for each record (each file). For records in *Compliance* mode, the *Retain Until Date* can be extended, but cannot be shortened.

- ▶ The following table summarizes how the *Retain Until Date* is determined, based on (a) the retention controls transmitted with the record (columns with orange highlighted headings) and (b) the *File Retention* default values configured for the View (columns with blue highlighted headings).
 - When a *Retain Until Date* is applied to the record, the View's *File Retention Mode* is also applied.
- Reminder: For the scope of this assessment, the View's *File Retention Mode* must be set to *Compliance*.

Read-Only ¹⁰	Atime ¹¹	Retain Until Date, with View configurations: • <u>No Default Retention Period</u> • <u>No Autocommit Grace Period</u>	Retain Until Date, with View configurations: • <u>With Default Retention Period</u> • <u>No Autocommit Grace Period</u>	Retain Until Date, with View configurations: • <u>With Default Retention Period</u> • <u>With Autocommit Grace Period</u>
Yes	Future	Atime value sets the <i>Retain Until Date</i>	Atime value sets the <i>Retain Until Date</i> (unless Min/Max guardrails are <u>not</u> met) If Min/Max are configured, but are <u>not</u> met, the <i>Retain Until Date</i> is calculated as follows: • If Atime is less than the calculated <i>Minimum Retention Period</i> : Record's last modified timestamp + Minimum Retention Period • If Atime is greater than the calculated <i>Maximum Retention Period</i> : Record's last modified timestamp + Maximum Retention Period	
No	Future	Same as row above	Same as row above	After autocommit grace period expires, then retention is set as described in the row above
Yes	Past	<u>Rejected</u> ; error returned; record creation operation <u>fails</u>	The record's last modified timestamp + Default Retention Period sets the <i>Retain Until Date</i>	The record's last modified timestamp + Default Retention Period sets the <i>Retain Until Date</i>
No	Past	Record is stored with <u>no</u> retention controls	Same as row above	After autocommit grace period expires, the record's last modified timestamp + Default Retention Period sets the <i>Retain Until Date</i>

- ▶ The preceding table explains the retention controls applied during record creation/storage.
- ▶ In addition, for previously stored records, retention controls may be modified, with certain limitations, as described in the following table.

¹⁰ When using SMB, the Boolean read-only attribute can be set. With NFS, read-only is enabled when the write permission is removed from the access control list (ACL).

¹¹ Atime (a.k.a., last access time) is transmitted with the record (file) and is evaluated when setting the records' *Retain Until Date*.

	File Retention Controls (WORM-enabled Views configured for NFS and/or SMB storage protocols)
Changing Retention mode	- The <i>File Retention Mode</i> is configured for the View and applied (stored) for each separate record. Once the <i>File Retention Mode</i> is stored for the record, it <u>cannot</u> be changed using the NFS or SMB protocols. - For information on changing the <i>File Retention Mode</i> for the View, which applies to records stored in the future, see Section 2.2.3.2, <i>View Capabilities and View Retention Configurations</i>.
Changing Retain Until Date	- When the <i>File Retention Mode</i> is set to <i>Compliance</i> for a record, the <i>Retain Until Date</i>: <u>cannot</u> be shortened (decreased). <u>cannot</u> be removed. <u>can</u> be lengthened (extended). - To extend the <i>Retain Until Date</i>, the NFS or SMB Protocol sends an <i>Atime</i> date that is further in the future. The <i>Atime</i> value is stored as the updated <i>Retain Until Date</i>. - Extending a record's <i>Atime</i> and <i>Retain Until Date</i> does <u>not</u> affect the value of the record's last modified timestamp.
Removing retention controls	Retention controls set to <i>Compliance</i> mode <u>cannot</u> be removed from a record.

2.2.3.3.2 Applying S3 Retention Controls

- ▶ For *WORM-enabled Views* configured with *S3 Retention* and the S3 protocol, a record is an individual version of an object. Each record is uniquely identified, within the bucket where it is stored, by the object name and version identifier. Versioning is automatically enabled and cannot be turned off.
 - By design, the record version's contents are retained immutably over its lifespan.
 - Record version metadata includes:
 - ◆ Immutable (unchangeable) metadata: Tenant, bucket name, object name and version identifier, custom metadata attributes, and creation/storage timestamp, as well as *Compliance* mode after it is applied.
 - ◆ Mutable (changeable) metadata: *Retain Until Date* (which can be extended, but not shortened), legal hold status, and user-defined S3 tags, and other attributes in the VAST 'Share-Everything' Metadata Store.
- ▶ For *WORM-enabled Views* configured with *S3 Retention* and the S3 protocol, two retention attributes are separately stored for each record version with retention controls:
 1. *S3 Retention Mode*: Once set to *Compliance*, the mode cannot be changed to *Governance* or removed.
 2. *Retain Until Date*: Once set to *Compliance* mode, the *Retain Until Date* can be extended, but cannot be shortened.
- ▶ The following table summarizes the retention controls (*S3 Retention Mode* and the *Retain Until Date*) applied during the initial storage process, based on (a) the *S3 Retention* attributes transmitted with the record version (columns with orange highlighted headings), (b) the *S3 Retention* default values configured for the View (columns with blue highlighted headings). Reminder: For this assessment, the *S3 Retention Mode* must be set to *Compliance* for the record version.

Transmitted S3 Retention Mode	Transmitted Retain Until Date	Record Version's Retention Controls, when the View does <u>not</u> have default retention settings	Record Version's Retention Controls, when the View <u>has</u> default retention settings
Null	mm/dd/yyyy	Error returned; record creation operation <u>fails</u>	
Null	Null	Record version is stored <u>without</u> retention controls	Record version is set to the View's <i>Default Retention Mode</i> (e.g., <i>Compliance</i>) and <i>Retain Until Date</i> is record version's creation/storage timestamp + View's Default Retention Period
<i>Governance</i>	mm/dd/yyyy	Record version is set to <i>Governance</i> mode and <i>Retain Until Date</i> is mm/dd/yyyy	
<i>Governance</i>	Null	<u>Rejected</u> ; error returned; record creation operation <u>fails</u>	
<i>Compliance</i>	mm/dd/yyyy	Record version is set to <i>Compliance</i> mode and <i>Retain Until Date</i> is mm/dd/yyyy	
<i>Compliance</i>	Null	<u>Rejected</u> ; error returned; record creation operation <u>fails</u>	

- ▶ The preceding table explains the retention controls applied during record creation/storage. In addition, retention controls may be applied to existing records, as described in the following table, in the row labeled **Modifying the retention controls**.
- ▶ The following describes the process of applying or changing retention controls on existing records, as well as limits related to modifying current retention controls.

	S3 Retention Controls (<i>WORM-enabled Views</i> configured for the S3 protocol)
Modifying or removing the retention controls	The S3 <i>Retention Mode</i> and <i>Retain Until Date</i> must be submitted as a <u>pair</u>. If only one attribute is transmitted, the operation <u>fails</u> and an error is reported. - For record versions previously set to <i>Compliance</i> mode, <u>authorized users</u>: <u>cannot</u> be changed from <i>Compliance</i> to <i>Governance</i>. <u>Cannot</u> remove <i>Compliance</i> (<u>cannot</u> change to <i>Null</i>). <u>Can</u> lengthen (extend), but <u>cannot</u> shorten or remove, the <i>Retain Until Date</i>. - If the version identifier is explicitly identified, the updated retention attributes are applied to the explicit record version. - If the version identifier is <u>not</u> explicitly identified, the updated retention attributes are applied to the current (top) record version. - Changing the retention attributes does <u>not</u> generate a new version and does <u>not</u> affect the record version's creation/storage timestamp.
Removing retention controls	Retention controls set to <i>Compliance</i> mode <u>cannot</u> be removed or cleared from a record version.

2.2.3.3.3 Record Operations and Retention Controls

- ▶ The following table describes the retention controls separately applied to: (1) records in *WORM-enabled Views* configured for *File Retention* applied in *Compliance* mode and (2) record versions in *WORM-enabled Views* configured for *S3 Retention* applied in *Compliance* mode.

- The first portion of the table lists controls for **View-level operations**, followed by controls for **Record-level operations and activities**.

	1. <i>File Retention</i> applied in <i>Compliance</i> mode	2. <i>S3 Retention</i> applied in <i>Compliance</i> mode
View-level operations		
Changing Paths	All attempts to change the View's storage path (directory) are <u>disallowed</u>.	
Modifying protocol selection	With <i>File Retention</i>, only NFS and SMB protocols are supported. All attempts to configure the S3 protocol are <u>disallowed</u>.	With <i>S3 Retention</i>, only the S3 protocol is supported. All attempts to change the protocol are <u>disallowed</u>.
Modifying data storage endpoints	- All attempts to change the existing SMB share name of the data storage endpoint is <u>disallowed</u>. - The NFS alias is optional and may be changed between <i>Null</i> and an alias, at any time. If the NFS alias is cleared, the storage path can be used to locate the View.	All attempts to change the S3 bucket name are <u>disallowed</u>.
Deleting Views	The View cannot be deleted unless it is empty.	
Record-level operations		
Uniquely identifying records	The unique identifier for a record is immutable and is the combination of tenant, full path (under the tenant) and file name.	The unique identifier for a record version is immutable and is the combination of tenant, bucket name (within the tenant), object name and version identifier.
Changing records' names	All attempts to change a record name are <u>rejected</u>.	- All attempts to change a record name (object name) are <u>rejected</u>. - Additionally, version identifiers are system-generated and are immutable.
Changing permissions	- Read permissions to a record may be changed (expanded or contracted) at any time. - Write permissions are <u>disallowed</u>.	
Tiering storage classes	Not applicable, the VAST DataStore is a single tier storage platform, by design.	
Accessing records and record versions	- Each record is uniquely identified and can be accessed separately. - Versioned records do <u>not</u> apply, since <i>File Retention</i> uses NFS and SMB protocols, which do <u>not</u> support the concept of versioned files. - Also see Section 2.4, <i>Capacity to Download and Transfer Records and Location Information</i>.	- Each record <u>version</u> is uniquely identified and can be accessed separately. - If the record is accessed <u>without</u> specifying the version identifier, the current (top) version is retrieved. If the current version is a Delete Marker, S3 proceeds as if the record does <u>not</u> exist. - Also see Section 2.4, <i>Capacity to Download and Transfer Records and Location Information</i>.
Displaying retention controls	The VAST Catalog query results may include: (a) <i>File Retention Mode</i>, (b) <i>Retain Until Date</i>, (c) legal hold status.	In addition to the VAST Catalog, the S3 <i>GetObject</i> and <i>HeadObject</i> results include: (a) <i>S3 Retention Mode</i>, (b) <i>Retain Until Date</i>, (c) legal hold status.

	1. File Retention applied in Compliance mode	2. S3 Retention applied in Compliance mode
Record-level activities		
Storing records or record versions	Versioned records do <u>not</u> apply, since <i>File Retention</i> uses NFS and SMB protocols, which do <u>not</u> support the concept of versioned files.	- Versioning must be <u>enabled</u>; accordingly: - If the object name is unique, it is stored as the first version of a new record. - If the object name is <u>not</u> unique, a new version is stored, with a new version identifier.
Modifying or overwriting records and associated metadata	- Each <u>record</u> and its immutable metadata are immutably stored for its lifespan. - All attempts to modify the contents of a record or overwrite a record, during its lifespan, are <u>rejected</u>. - After retention controls expire and any legal hold is cleared (removed), the record may be deleted, but <u>cannot</u> be modified.	- Each <u>record version</u>, together with its immutable metadata, is immutably stored for its lifespan. - All attempts to modify the contents of a record version, during its lifespan, are <u>rejected</u>. - Attempts to overwrite an existing record or store a new record with the same name as one that already exists in the bucket, results in storing a new version, with separately applied retention controls and <i>legal hold</i> status. - After retention controls expire and any legal hold is cleared (removed), the record version may be deleted, but <u>cannot</u> be modified.
Changing legal hold status	A record's legal hold status <u>can</u> be set (Yes) or cleared (No), whether or not it has retention controls are applied. See Section 2.2.3.4, <i>Legal Holds (Temporary Holds)</i>, for additional information.	
Restricting deletion	- All attempts to delete a record, prior to the expiration of the <i>Retain Until Date</i> and clearing of any legal hold, are <u>rejected</u>. - See Section 2.2.3.5, <i>Deletion Controls</i>, for additional information.	- All attempts to delete a record version, prior to the expiration of the <i>Retain Until Date</i> and clearing of any legal hold, are <u>rejected</u>. - All attempts to delete a record without specifying the version identifier results in appending a delete marker as the current (top) version. The delete marker can be removed to recover the record. - Privileged delete (i.e., <i>BypassGovernanceRetention</i>) command <u>cannot</u> be used to prematurely delete record versions protected by <i>S3 Retention</i> in <i>Compliance</i> mode. - See Section 2.2.3.5, <i>Deletion Controls</i>, for additional information.
Copying records	- A record may be copied to a different storage path (i.e., directory). - The creation timestamp of the copy reflects the date and time that the copy is stored in the destination location (not the date and time the record was originally stored in the source location). - Retention controls and the legal hold status must be separately applied to the new copy, in accordance with the configurations of the View where the new copy is stored. - A record cannot be copied to a different tenant. (Tenants are independent and are unaware of other tenants.)	
Moving records	A record <u>cannot</u> be moved to a different path (i.e., directory).	

2.2.3.4 Legal Holds (Temporary Holds)

When a record is subject to preservation requirements for subpoena, litigation, regulatory investigation or other special circumstances, it must be preserved immutably, i.e., any deletion, modification or overwrite must be prohibited until the hold is clear (No).

- ▶ Legal hold features are available for records accessible by *WORM-enabled Views*. Legal hold features are not available for snapshots.
- ▶ The following table separately describes the legal hold features for: (1) records in *WORM-enabled Views* configured for *File Retention* and (2) record versions in *WORM-enabled Views* configured for *S3 Retention*.

	1. File Retention	2. S3 Retention
Applying and clearing legal holds	- Using VMS, the legal hold status may be set (Yes) or cleared (No) from any <u>record</u> (non-versioned file) stored in a <i>WORM-enabled View</i> configured for the NFS or SMB protocols. - The legal hold status is independent of the <u>record's Retain Until Date</u> and <i>File Retention Mode</i>; therefore, a legal hold status may be applied to <u>any record</u> in a <i>WORM-enabled View</i> whether or not the record has retention controls. - If the VMS user does <u>not</u> have the required permissions, the action is <u>rejected</u>.	- Using VAST's S3-compatible APIs, the legal hold status may be set (Yes) or cleared (No) from <u>any record version</u> stored in a <i>WORM-enabled View</i> configured for the S3 protocol. The legal hold status must be set or cleared for each record version. - If no version is specified, the legal hold status is applied to the current (top) version and if the current (top) version is a Delete Marker, the legal hold status is <u>not</u> updated. - The legal hold status is independent of the <u>record version's Retain Until Date</u> and <i>S3 Retention Mode</i>; therefore, a legal hold status may be applied to <u>any record version</u> in a <i>WORM-enabled View</i> whether or not the record version has retention controls. - If the user does <u>not</u> have the required permissions, the action is <u>rejected</u>.
Legal hold protections	- When the legal hold status is set (Yes) for a specific <u>record</u>, deletion of the <u>record</u> is <u>prohibited</u> until the legal hold status is clear (No). - When the legal hold status is clear (No), this attribute no longer mandates preservation of the <u>record</u>; however other retention controls continue to be enforced for the <u>record</u>.	- When the legal hold status is set (Yes) for a specific <u>record version</u>, deletion of the <u>record version</u> is <u>prohibited</u> until the legal hold status is clear (No). - When the legal hold status is clear (No), this attribute no longer mandates preservation of the <u>record version</u>; however other retention controls continue to be enforced for the <u>record version</u>.
Displaying retention controls	- The VAST Catalog query results may include legal hold status. - In addition, users may also get the legal hold status from VMS.	- The VAST Catalog query results may include legal hold status. - In addition, the S3 <i>GetObject</i>, <i>HeadObject</i> and <i>GetObjectLegalHold</i> results include legal hold status.

2.2.3.5 Deletion Controls

- The following table separately describes deletion for: (1) records in *WORM-enabled* Views configured for *File Retention*, in *Compliance* mode and (2) record versions in *WORM-enabled* Views configured for *S3 Retention* in *Compliance* mode.

	1. <i>File Retention</i> applied in <i>Compliance</i> mode	2. <i>S3 Retention</i> applied in <i>Compliance</i> mode
Determining eligibility for deletion	- The <u>record</u>, together with its metadata, are eligible for deletion only after the two following conditions are met: - The <i>Retain Until Date</i> is expired (is in the past). - The legal hold status is clear (No).	- The <u>record version</u>, together with its metadata, are eligible for deletion only after the two following conditions are met: - The <i>Retain Until Date</i> is expired (is in the past). - The legal hold status is clear (No).
Restricting deletion of records and record versions	Actions by authorized users to delete an <u>ineligible record</u> with either an <u>unexpired</u> <i>Retain Until Date</i> or a legal hold status (Yes), are <u>rejected</u>.	- Actions by authorized users to delete an <u>ineligible record version</u> with either an <u>unexpired</u> <i>Retain Until Date</i> or a legal hold status (Yes), are <u>rejected</u>. - Actions by authorized users to delete an <u>ineligible record</u> (without specifying the version identifier), results in appending a delete marker as the current (top) version. <u>Note</u>: Delete markers can be removed, which results in reinstating or recovering the deleted (hidden) record.
Deleting eligible records and record versions	Actions by authorized users to delete an <u>eligible record</u> with an <u>expired</u> <i>Retain Until Date</i> and a clear legal hold status (No), results in record deletion.	- Actions by authorized users to delete an <u>eligible record version</u> with an <u>expired</u> <i>Retain Until Date</i> and a clear legal hold status (No), results in record deletion. - Actions by authorized users to delete an <u>eligible record</u> (without specifying the version identifier), results in appending a delete marker as the current (top) version. <u>Note</u>: Delete markers can be removed, which results in reinstating or recovering the deleted (hidden) record.
Using privileged delete	Not applicable, since privileged delete features are not available.	Privileged delete (i.e., <i>BypassGovernanceRetention</i>) command <u>cannot</u> be used to prematurely delete record versions protected by <i>S3 Retention</i> in <i>Compliance</i> mode.
Deleting Directories or Views	A <i>WORM-enabled</i> View must be empty before it can be deleted. Accordingly, deleting a View to effectuate the premature deletion of records is <u>prohibited</u>.	

2.2.3.6 Snapshot Configurations, Retention Controls and Deletion

- ▶ **Protection Policies** create **snapshots**, which are read-only and serve as virtual point-in-time archive copies of the directory the policy protects. By design, each snapshot is (a) immutable, (b) inextricably linked to its source directory (i.e., the storage path it protects) and its Protection Policy, and (c) identified by system-generated immutable snapshot creation timestamp.
- ▶ In addition, VAST developed an *Indestructibility* feature for VAST clusters¹².
 - When the cluster's Indestructibility feature is enabled, the Protection Policies and the associated snapshots can be set as *indestructible*. When this combination of *Indestructibility* features is applied and enforced, modification and deletion of the Protection Policies and snapshots is prohibited.
 - The cluster's *Indestructibility* feature may be suspended for a time-limited period (e.g., 1 hour), using a token obtained from VAST Data support personnel. Note: The regulated entity can stipulate that either one or two administrators must authenticate with VAST Data support personnel to request a token.
 - ◆ When the cluster's *Indestructibility* feature is suspended, the Protection Policies and snapshots can be modified and deleted, i.e., the Protection Policies and snapshots are unlocked, though they may remain marked as *indestructible*.
- ▶ The following two subsections describe the configurations and retention controls for locked and unlocked Protection Policies and Snapshots.

2.2.3.6.1 Protection Policy Configurations and Retention Controls

- ▶ **Protection Policy** configurations include:
 - Policy name, source directory (i.e., protected storage path), destination of the snapshot.
 - **Snapshot schedules**, which stipulate:
 - ◆ Frequency of creating snapshots, which is set in seconds, minutes, hours or days.
 - ◆ Retention period for the local copy, which is set in seconds, minutes, hours or days.
 - ◆ Retention period for the remote copy, which is set in seconds, minutes, hours or days.
 - *Indestructible* option must be set. (Note: This *Indestructible* option for the Protection Policy is in addition to enabling the *Indestructibility* feature for VAST cluster, described preceding subsection. When the cluster's Indestructibility feature is enforced, the Protection Policy is locked. When the cluster's Indestructibility feature is suspended, the Protection Policy is unlocked, even though the *Indestructible* option is set.)
- ▶ While in the locked state, the Protection Policy cannot be deleted and its configurations cannot be changed, except that the retention period set in the snapshot schedule may be extended. Changes only apply to new snapshots created after the change.

¹² A VAST cluster is the set of VAST Servers and VAST Enclosures that make up a single management domain and namespace.

- ▶ While in the unlocked state, the Protection Policy can be deleted and its configurations can be changed, e.g., the retention period set for the snapshot schedule may be shortened or extended and a snapshot schedule may be removed. Changes only apply to new snapshots created after the change.

2.2.3.6.2 [Snapshot Configurations and Retention Controls](#)

- ▶ While in the locked state, the snapshot metadata includes:
 - Immutable (unchangeable) metadata: Snapshot name, directory (i.e., protected storage path), creation timestamp, type (local copy or remote copy), Protection Policy that created the snapshot and *Indestructible* value (Yes/No).
 - Mutable (changeable) metadata: *Snapshot Expiry Timestamp*.
- ▶ Each snapshot inherits the configurations of the Protection Policy at the time of snapshot creation.
 - The *Snapshot Expiry Timestamp* is (a) calculated by adding the retention period stipulated in the Protection Policy to the snapshot creation date and (b) stored as metadata of the snapshot.
 - The Protection Policy's *Indestructible* option is inherited by the snapshot. (*Note*: This *Indestructible* option applied to a snapshot is in addition to enabling the *Indestructibility* feature for VAST cluster. When the cluster's Indestructibility feature is enforced, the snapshot is locked. When the cluster's Indestructibility feature is suspended, the snapshot is unlocked, even though the *Indestructible* option is set.)
- ▶ While in the locked state, the snapshot cannot be deleted and its configurations cannot be changed, except that the *Snapshot Expiry Timestamp* may be extended.
- ▶ While in the unlocked state, the snapshot can be deleted and its configurations can be changed, e.g., the *Snapshot Expiry Timestamp* may be shortened or extended. Therefore, procedural controls and monitoring are required to scrutinize administrative actions taken when snapshots are unlocked.
- ▶ Legal hold features are not available for snapshots. Therefore, if a snapshot requires preservation for legal matters, government investigations, external audits and other similar circumstances, either extend the *Snapshot Expiry Timestamp* or protect the snapshot via cloning or another method.
- ▶ The snapshot *revert* feature is automatically disabled for snapshots that include the contents of *WORM-enabled Views*. *Note*: If the *revert* feature were enabled, the current directory would be overwritten by the snapshot.

2.2.3.7 [Security](#)

In addition to the stringent retention and management controls described above, the VAST solution provides the following security capabilities, which support the authenticity and reliability of the records.

- ▶ For the [View Management System](#), role based access control (RBAC) security and identity and access management policies are used to manage users and associated create, view, edit, and delete permissions. Permissions may be assigned to security groups, called roles, and to managers.
- ▶ Permissions to set and view *File Retention* and *S3 Retention* configurations on the View and record level are controlled by identity-based policies and View configurations.

- View configurations define security settings that control access to the records, such as defining whether NFS (POSIX) or SMB access control lists (ACLs) are used to control permissions, restricting types of access by host Internet Protocol or choosing a security flavor¹³ which determines cross protocol behavior for handling permissions for users and groups to access files or objects.
- Permission repair is disallowed on WORM-enabled Views, to avoid the possibility of adding a new access control entry (ACE) with write permissions.
- ▶ Encryption features may be enabled to transparently [encrypt and decrypt data at rest](#) using 256-bit AES-XTS encryption. (Encryption is disabled by default.) When enabled, records and metadata are encrypted as the data is stored, ensuring confidentiality of data at rest.
 - Also, the VAST solution is capable of [encrypting data in transit](#) between certain internal network connections.
- ▶ Audits by independent third-parties and internal staff are undertaken on a regular basis to verify security, privacy and compliance controls.

2.2.3.8 Clock Management

- ▶ During install, VAST clusters are configured for external NTP clock sources, which cannot be removed.
- ▶ The VAST system disallows manual adjustments to its clock time and automatically synchronizes time with a network protocol (NTP) clock to ensure that the local clock is within a 5 minute threshold.
 - In the event the VAST solution system clock and the NTP clock are out of sync by more than 5 minutes, the VAST solution system triggers an alert and blocks deletions of all records with retention controls, whether or not the record is eligible for deletion.
 - Only VAST Data support personnel are authorized to reset the VAST solution system clock and unblock deletion of eligible records.
- ▶ This process ensures that timestamps are accurately recorded when the record and metadata are written, and it ensures that the clock cannot be temporarily advanced to allow premature record deletion.

2.2.4 Additional Considerations

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

- ▶ *Enabling WORM* and properly configuring *File Retention* and *S3 Retention* features on Views that will store records. Note: Cohasset recommends configuring optional default retention settings to assure retention controls are applied to all records stored in the View.
- ▶ Ensuring that the retention controls meet regulators' retention requirements and are properly applied to records. Reminder: Features, configurations and requirements for *File Retention* and *S3 Retention* differ, plus changes to default configurations apply to records stored after the change is made; therefore, care must be taken to configure, use and monitor *WORM-enabled* Views and stored records.

¹³ The security flavor determines which protocol's permission checking algorithm is used, which protocols are allowed to set permissions on files and directories and how initial permissions are set on new files and directories.

- ▶ Ensuring all records required for compliance with the Rules are successfully stored with either *File Retention* or *S3 Retention* controls, preferably within 24 hours of creation.
- ▶ Storing records requiring event-based¹⁴ retention periods in a separate compliant system, since the VAST DataStore does not currently support event-based retention periods.
- ▶ Setting the legal hold status or otherwise protecting records that require preservation for legal matters, government investigations, external audits and other similar circumstances and clearing legal holds when the matter is released.
- ▶ Establishing and maintaining appropriate security controls and enabling encryption of data at rest, when appropriate.
- ▶ Ensuring that NTP clock servers are appropriately configured and monitored.

Additionally, for snapshots that will be retained for regulatory compliance, the regulated entity is responsible for:

- ▶ Configuring the *Indestructibility* feature for the cluster and Protection Policies, which will be inherited by the snapshots.
- ▶ Generating snapshots at least once every 24 hours (to assure a daily record is retained), setting retention controls that meet regulatory requirements retention requirements and assuring that the retention controls are not circumvented, since authorized users may obtain a time-limited *token* issued by VAST Data support personnel, which allows Protection Policy and snapshot configurations to be modified and snapshots to be deleted before the *Snapshot Expiry Timestamp*. Note: Since retention controls for snapshots are less-restrictive and can be circumvented, procedural controls and monitoring must be established to scrutinize administrative actions.
- ▶ Extending the *Snapshot Expiry Timestamp* or otherwise protecting snapshots that require preservation for legal matters, government investigations, external audits and other similar circumstances.

Further, the regulated entity is responsible for: (a) authorizing user permissions and (b) maintaining appropriate hardware and software, encryption keys, and other information and services needed to retain the records.

2.3 Record Storage Verification

2.3.1 Compliance Requirement

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.

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

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

¹⁴ 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.

2.3.2 Compliance Assessment

Cohasset affirms that the functionality of the VAST DataStore 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 VAST DataStore Capabilities

The recording and post-recording verification processes of the VAST DataStore are described below.

2.3.3.1 Recording Process

- ▶ When records are initially recorded the transmitted data is erasure encoded and stored on high-capacity solid-state drives.
 - The VAST DataStore uses locally decodable erasure codes, which are a class of forward error-correcting codes that can be used to detect and correct a limited number of errors in transmitted data without the need for retransmission.
 - CRC (cyclic redundancy check) checksums are calculated and stored as immutable pointers to stored data.
- ▶ Snapshots of directories are represented by marking existing records at the snapshot's designated timestamp.

2.3.3.2 Post-Recording Verification Process

- ▶ The VAST DataStore employs background processes to continuously scan the storage environment and check for errors, using the checksums.
- ▶ During retrieval, checksums are used to confirm record integrity and ensure that an accurate record is delivered.
- ▶ If data is corrupt, the VAST DataStore reconstructs the data from non-corrupt erasure coded stripes.

2.3.4 Additional Considerations

The source system is responsible for transmitting the complete contents of the required records and the VAST DataStore validates the accuracy of the recording process.

2.4 Capacity to Download and Transfer Records and Location Information

2.4.1 Compliance Requirement

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

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

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]

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

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

2.4.2 Compliance Assessment

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

2.4.3 VAST DataStore Capabilities

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

- ▶ Each record's unique identifier is immutable and facilitates findability.
 - For records (files), when using the NFS or SMB protocols, the immutable unique identifier is the combination of tenant, full path and file name.
 - For record versions (object versions), when using the S3 protocol, the immutable unique identifier is the combination of tenant, bucket name, object name and version identifier.
- ▶ In addition, the applicable last modified and creation/storage timestamps are immutable when retention controls are applied.
- ▶ Records may be located using a variety of methods:
 1. Authorized users may traverse the directory and file structure.
 2. Protocol-specific lookup operations can be used to access stored records and metadata attributes.
 3. Authorized users may query the VAST Catalog using simple SQL queries.
 - ◆ The Catalog compiles the attributes related to the various supported protocols (NFS, SMB, and S3) and enables high performance querying of the contents of the current View of records (files, objects and versions of objects) and directories.
 - ◆ Over 25 attributes may be queried, including, but are not limited to:
 - Full path,
 - File name,
 - Creation/storage, last modified and last access timestamps, and
 - Retention attributes, i.e., *Retain Until Date*, *Read-Only* attribute and *legal hold* status.
 - ◆ Query results may be exported as standard comma separated value (CSV) files and the downloaded file may be accessed locally.
 - ◆ Authorized storage administrators can query the Catalog through VMS, and other authorized users can query the Catalog through the Big Catalog CLI or connected third party query engines.

- ▶ Selected records and the Catalog query results may be downloaded to a specified location, then local capabilities may be used to transfer the records, as requested by the regulator.

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

- ▶ Snapshots are virtual point-in-time archive copies of any directory. Each archive copy is:
 - Inextricably linked to the original source directory that was archived.
 - Separately identified by snapshot identifier (clone identifier), and the snapshot timestamp.
 - Organized consistent with the original source, i.e., organized by directories and folders.
- ▶ Snapshots may be accessed using the following two methods:
 1. Traverse the directory and select an associated (linked) snapshot, which is listed in a timestamped hierarchy. Then, access and copy or download a specific snapshot of a record. (Note: This feature must be enabled by the administrator.)
 2. Select a snapshot and create a clone (duplicate of the source directory) on a specified destination. The clone has the same structure and metadata as the source, except that it is stored in a new location with a unique top path name. Authorized users may access the clone similar to other directories.

Note: The *revert* feature, which is a third method of accessing a snapshot, is automatically disallowed for snapshots that include the contents of *WORM-enabled* Views. If the *revert* feature were enabled, the selected directory would be overwritten by the snapshot.

2.4.4 Additional Considerations

Additionally, the regulated entity is responsible for: (a) authorizing user permissions, (b) maintaining appropriate technology and resource capacity, encryption keys, and other information and services needed to use the VAST DataStore to readily access, download, and transfer the records and the information needed to locate the records, and (c) 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]

- ▶ 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 the VAST DataStore meets the requirement in SEC Rules 17a-4(f)(2)(v)(B) and 18a-6(f)(2)(v)(B) by retaining a persistent alternate source to reestablish the records through the use of erasure coding, when the considerations described in Section 2.5.4 are satisfied.

2.5.3 VAST DataStore Capabilities

- ▶ For compliance with paragraph (B), when records are initially recorded, the VAST DataStore automatically erasure codes data and stores it on high-capacity solid-state drives.
 - The VAST DataStore uses locally decodable erasure codes that are a class of forward error-correcting codes that can reconstruct erased data, like the data on a failed drive, using only a small fraction of the surviving data stripes.
- ▶ Snapshots of directories are represented by marking records as they existed at the snapshot’s designated timestamp; therefore, the snapshots are protected by the same erasure coding features.

2.5.4 Additional Considerations

Additionally, the VAST replication service can be set to create and maintain a replicated mirror according to policy configurations, which set the frequency and retention duration.

Also, the regulated entity is responsible for maintaining the technology, storage capacity, encryption keys, and other information and services needed to use the VAST DataStore and permit access to redundant records.

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

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

2.6 Audit System

2.6.1 Compliance Requirement

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

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

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

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

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

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

2.6.2 Compliance Assessment

Cohasset asserts that the VAST DataStore, in conjunction with the VAST Audit Log, when enabled, supports the regulated entity's efforts to meet this SEC requirement for an audit system.

2.6.3 VAST DataStore Capabilities

The regulated entity is responsible for an audit system, and compliance is supported by the VAST DataStore.

- ▶ For each record in a *WORM-enabled View*, the following attributes are immutably retained for the same time period as the record. These attributes provide valuable audit information.
 - Unique Identifier, which is the combination of (a) tenant, full path and file name for NFS and SMB protocols and (b) tenant, bucket name, object name and version identifier for S3 protocols.
 - Creation/storage and last modified timestamps, which are system-generated and cannot be modified by a user.
- ▶ A snapshot is inextricably linked to its source directory and is assigned a system-generated creation timestamp. Further, each record in the snapshot maintains its unique identifier, creation/storage time stamp and last modified timestamp. These attributes provide valuable audit information.
- ▶ The record content in the directory (i.e., storage path) of a *WORM-enabled View* or a snapshot cannot be changed; each record is immutably stored over its lifespan. Specifically:
 - After applying retention controls, the NFS and SMB protocols disallow modifications and overwrites.
 - The S3 protocol disallows modifications and overwrites over the lifespan of the record version, by design. Any attempt to modify the contents or overwrite the object results in a new version.
 - A snapshot is a point-in-time archive that is immutable during the lifespan of the snapshot.

Accordingly, tracking of the inputting of changes made to the record content is not relevant to the VAST DataStore.

- ▶ In addition, the VMS Audit Log may be enabled to capture an audit event of the user and timestamp of certain successful and failed configurations and record-related operations (e.g., creation, deletion, read and write operations, permission changes, and applying retention controls and legal holds, among other activities).
 - For a VAST cluster, the availability period for audit entities may be configured to a specified period of time or *Forever*. During the availability period the VMS Audit Log can be viewed, searched and exported.
 - The VAST Audit Log is accessible using the VAST GUI.
 - Audit events may be exported to a CSV file and may be ingested into external applications such as security information and event management tools.

2.6.4 Additional Considerations

The regulated entity is responsible for maintaining an audit system for inputting records. In addition to relying on the immutable metadata, the regulated entity may utilize VMS Audit Log 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 the VAST DataStore, as described in Section 1.3, *VAST DataStore Overview and Assessment Scope*, in comparison to CFTC electronic regulatory record requirements. Specifically, this section associates the features described in Section 2, *Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e)*, with the principles-based requirements of CFTC Rule 1.31(c)-(d).

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

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

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

In Section 2 of this report, Cohasset assesses both:

1. *File Retention* and *S3 Retention*, when in *Compliance* mode, which is a highly restrictive configuration that assures the storage solution applies integrated controls to (a) protect immutability of the record content and certain system metadata and (b) prevent deletion over the applied retention period.
2. *Locked* snapshots, e.g., virtual point-in-time archive copies of any directory that have less-restrictive retention controls applied.

The following table pertains specifically to *File Retention* and *S3 Retention* and correlates the functionality of the VAST DataStore, using *File Retention* and *S3 Retention*, when in *Compliance* mode, 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 the VAST DataStore, using the less restrictive *Governance* mode, meets these *principles-based* CFTC requirements, when the regulated entity applies appropriate procedural controls to scrutinize actions taken that may allow content to be modified or deleted prior to expiration of the retention period. This less restrictive *Governance* mode provides flexibility to remove or shorten retention periods, which

¹⁷ 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.

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 the VAST DataStore, with *File Retention* and *S3 Retention* to meet the requirements for electronic regulatory records in CFTC Rule 1.31(c)-(d).

CFTC 1.31(c)-(d) Regulation [emphasis added]	Compliance Assessment Relative to CFTC 1.31(c)-(d)
<i>(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:</i> <i>(1) Generally. Each records entity shall retain regulatory records in a form and manner that ensures the <u>authenticity and reliability</u> of such regulatory records in accordance with the Act and Commission regulations in this chapter.</i> <i>(2) Electronic regulatory records. Each records entity maintaining electronic regulatory records shall establish appropriate systems and controls that ensure the <u>authenticity and reliability</u> of electronic regulatory records, including, without limitation:</i> <i>(i) Systems that maintain the security, signature, and data as necessary to ensure the <u>authenticity</u> of the information contained in electronic regulatory records and to monitor compliance with the Act and Commission regulations in this chapter;</i>	It is Cohasset's opinion that the CFTC requirements in (c)(1) and (c)(2)(i), for records¹⁸ with time-based retention periods, are met by the functionality of the VAST DataStore, with either <i>File Retention</i> and <i>S3 Retention</i>, when in <i>Compliance</i> mode or <i>Governance</i> mode. This report describes the functionality of the VAST DataStore, with <i>File Retention</i> and <i>S3 Retention</i>, set to <i>Compliance</i> mode, in: • Section 2.2, <i>Non-Rewriteable, Non-Erasable Record Format</i> • Section 2.3, <i>Record Storage Verification</i> • Section 2.4, <i>Capacity to Download and Transfer Records and Location Information</i> • Section 2.6, <i>Audit System</i> Additionally, for <u>records stored electronically</u>, the CFTC definition of <u>regulatory records</u> in 17 CFR § 1.31(a) includes information to access, search and display records, as well as data on records creation, formatting and modification: <u>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:</u> <u>(i) Any data necessary to access, search, or display any such books and records; and</u> <u>(ii) All data produced and stored electronically describing how and when such books and records were created, formatted, or modified.</u> [emphasis added] The VAST DataStore retains immutable metadata attributes (e.g., Unique Identifiers and applicable creation/storage and/or last modified timestamps) as an integral component of the records, and, therefore, these attributes are subject to the same retention controls as the associated record. These immutable attributes support both (a) records access, search and display and (b) audit system and accountability for inputting the records. Additionally, mutable metadata attributes stored for records include retention controls and legal hold statuses. The most recent values of mutable metadata are retained for the same time period as the associated records. Further, the VAST DataStore in conjunction with the VMS Audit Log, when enabled, tracks audit events and provides storage options for retaining this additional audit system information. For additional information, see Section 2.6, <i>Audit System</i>.

¹⁸ The regulated entity is responsible for retaining and managing any additional required information, such as data on how and when the records were created, formatted, or modified, in a compliant manner.

CFTC 1.31(c)-(d) Regulation [emphasis added]	Compliance Assessment Relative to CFTC 1.31(c)-(d)
<i>(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</i>	It is Cohasset's opinion that the VAST DataStore capabilities described in Section 2.5, <i>Record Redundancy</i>, including a method of maintaining an alternate source to reestablish the records and associated system metadata, meet the CFTC requirements (c)(2)(ii) to <u>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</u>.
<i>(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.</i>	The regulated entity is required to create and retain an <i>up-to-date inventory</i>, as required for compliance with 17 CFR § 1.31(c)(iii).
<i>(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:</i> <i>(1) Inspection. All regulatory records shall be open to inspection by any representative of the Commission or the United States Department of Justice.</i> <i>(2) Production of paper regulatory records. ***</i> <i>(3) Production of electronic regulatory records.</i> <i>(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.</i> <i>(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.</i> <i>(4) Production of original regulatory records. ***</i>	It is Cohasset's opinion that the VAST DataStore 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, <i>Non-Rewriteable, Non-Erasable Record Format</i> ● Section 2.4, <i>Capacity to Download and Transfer Records and Location Information</i> ● Section 2.6, <i>Audit System</i>

4 • Conclusions

In Section 2 of this report, Cohasset assessed the functionality of the VAST DataStore¹⁹ (a) *File Retention* and *S3 Retention*, set to *Compliance* mode and (b) *locked* snapshots 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 the VAST DataStore, when properly configured with *File Retention* and *S3 Retention*, in *Compliance* mode, has the following functionality, which meets the regulatory requirements:

- ▶ Retains the records and immutable record metadata in non-rewriteable, non-erasable format for time-based retention periods by applying either *File Retention* or *S3 Retention*, in *Compliance* mode.
- ▶ Applies legal holds to preserve records (files and objects) for a subpoena, legal matters or similar circumstances, and permits clearing the hold when the matter is released.
- ▶ Prohibits deletion of records until the *Retain Until Date* is expired and any applied legal hold is clear (No).
- ▶ Verifies the accuracy of the process for storing and retaining the records, using both (a) checksums and the VAST DataStore validation processes and (b) forward error-correcting codes, which detect and correct transmission errors, eliminating the need for retransmission.
- ▶ Provides authorized users with the capacity and tools to readily (a) query record metadata to find records, (b) list the query results, and (c) download selected records and associated metadata attributes for a browser or other local tool to produce a human readable image and a reasonably usable electronic format.
- ▶ Maintains records redundancy to regenerate an accurate replica of the record from the erasure coded data should an error occur or an availability problem be encountered.
- ▶ Supports the regulated entity's obligation to retain an audit system for non-rewriteable, non-erasable records.

Accordingly, Cohasset concludes that the VAST DataStore, when properly configured with *File Retention* or *S3 Retention* 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 *File Retention* or *S3 Retention* capabilities meet the principles-based electronic records requirements of CFTC Rule 1.31(c)-(d). Note: For a description of the less-restrictive retention controls applied to *locked* snapshots, see Section 2.2.3.6, *Snapshot Configurations and Retention Controls*, and other sections of this report.

¹⁹ See Section 1.3, *VAST DataStore Overview and Assessment Scope*, for an overview of the solution and the scope of deployments included in the assessment.

Appendix A • Overview of Relevant Electronic Records Requirements

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

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

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

Effective January 3, 2023, the U.S. Securities and Exchange Commission (SEC) promulgated amendments²⁰ 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 and complete time-stamped audit-trail alternative and (b) allow regulated entities to continue using the electronic recordkeeping systems they currently employ to meet the non-rewriteable, non-erasable (i.e., WORM or write-once, read-many) requirement.

*Under the final amendments, broker-dealers and nonbank SBS Entities have the flexibility to preserve all of their electronic Broker-Dealer Regulatory Records or SBS Entity Regulatory Records either by: (1) using an electronic recordkeeping system that meets either the audit-trail requirement or the WORM requirement; or (2) preserving some electronic records using an electronic recordkeeping system that meets the audit-trail requirement and preserving other electronic records using an electronic recordkeeping system that meets the WORM requirement.*²² [emphasis added]

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

A.1.1 Record and Audit-Trail Alternative

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

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]

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

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

The Commission confirms that a broker-dealer or nonbank SBS Entity can rely on the 2003 and 2019 interpretations with respect to meeting the WORM requirement of Rule 17a-4(f) or 18a-6(e), as amended.

*In 2001, the Commission issued guidance that Rule 17a-4(f) was consistent with the ESIGN Act. The final amendments to Rule 17a-4(f) do not alter the rule in a way that would change this guidance. Moreover, because Rule 18a-6(e) is closely modelled on Rule 17a-4(f), it also is consistent with the ESIGN Act*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 SBS/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 the VAST DataStore related to each requirement.

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

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

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

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

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

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.

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.

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*