Cohasset Associates

Hitachi VSP One File

COMPLIANCE ASSESSMENT

SEC 17a-4(f), SEC 18a-6(e), FINRA 4511(c) and CFTC 1.31(c)-(d) and the MiFID II Delegated Regulation(72)(1)

Abstract

Hitachi Vantara's **Virtual Storage Platform (VSP) One File** is a highly secure storage platform for files and snapshots. Features offered as part of the appliance-based VSP One File solution are designed to meet securities industry requirements for preserving records in non-rewriteable, non-erasable format for the applied retention period.

In this report, Cohasset Associates, Inc. (Cohasset) assesses the functionality of VSP One File (see Section 1.3, *VSP One File 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);
- Commodity Futures Trading Commission (CFTC) in 17 CFR § 1.31(c)-(d); and
- The European Parliament and the Council of the European Union in Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing MiFID II (the MiFID II Delegated Regulation), Article 72(1).

It is Cohasset's opinion that VSP One File, when properly configured and used with the *Strict WORM File System* and *Snapshot Retention* features, meets the requirements for electronic recordkeeping set forth in the above Rules.

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.

February 2025

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

+1.312.527.1550 | www.cohasset.com

Table of Contents

1 • Introduction

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

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

1.1 Overview of the Regulatory Requirements

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

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

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

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

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

1.1.2 FINRA Rule 4511(c) Requirements

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

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

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

---

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

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

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

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

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

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

1.1.4 MiFID II Delegated Regulation(72)(1) Requirements

On January 3, 2018, *Directive 2014/65/EU*[4], Markets in Financial Instruments Directive II (MiFID II), became effective and established a definition of durable medium for recordkeeping to enable the client to store and access its information. As a supplement to MiFID II, the *Commission Delegated Regulation (EU) 2017/565*[5] *(the MiFID II Delegated Regulation),* Article 72(1), requires records to be *"retained in a medium that allows the storage of information in a way accessible for future reference by the competent authority"* and specifies the recordkeeping conditions that must be met.

For additional information, refer to Section 4, *Summary Assessment of Compliance with the MiFID II Delegated Regulation(72)(1),* and Appendix A.4, *Overview of the Medium* and *Retention of Records Requirements of MiFID II*.

1.2 Purpose and Approach

To obtain an independent and objective assessment of the compliance capabilities of VSP One File for preserving required electronic records, Hitachi Vantara 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.

Hitachi Vantara engaged Cohasset to:

- Assess the functionality of VSP One File, 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 VSP One File; see Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d);*

---

4 *Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments*.

5 *Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive*.

- Associate the requirements of Article 72(1) of the MiFID II Delegated Regulation with the assessed functionality of VSP One File; see Section 4, *Summary Assessment of Compliance with the MiFID II Delegated Regulation(72)(1);* 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 VSP One File and its functionality or other Hitachi Vantara products or services. The information utilized by Cohasset to conduct this assessment consisted of: (a) oral discussions, (b) system documentation, (c) user and system administrator guides, and (d) related materials provided by Hitachi Vantara 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 VSP One File Overview and Assessment Scope

1.3.1 VSP One File Overview

VSP One File is a highly secure storage platform for files and snapshots. The appliance-based solution provides a unified user interface for the configuration, monitoring and management of the platform. Offered as part of the VSP One File solution, the *Strict WORM File System* and *Snapshot Retention* features are designed to meet securities industry requirements for preserving electronic records[6] in non-rewriteable, non-erasable format in compliance with SEC Rules.

The logical storage architecture of VSP One File is depicted in Figure 1 and summarized as follows:

A **Namespace** acts as a distributed file system service, which points to different storage resources within the appliance, e.g., Virtual NAS servers and storage pools, and presents them as a single logical directory tree. Additionally, Namespaces may be configured to support muti-tenancy.

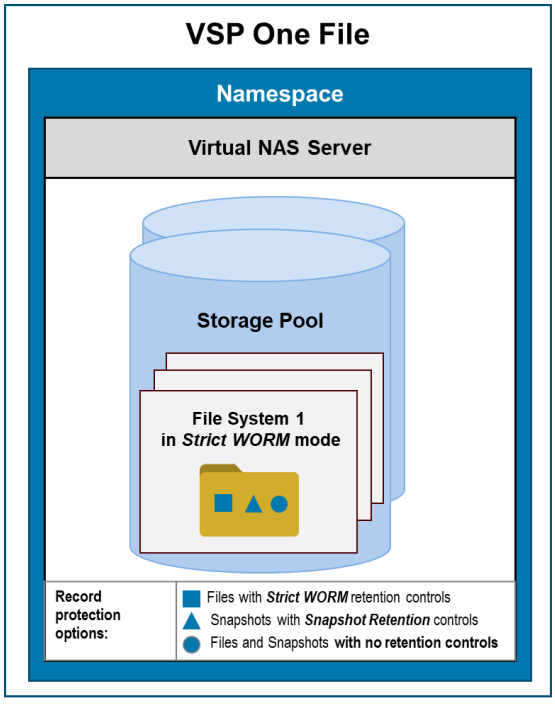

Figure 1: VSP One File Logical Storage Architecture

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

Within a Namespace, one or more **Virtual NAS Servers** provide server resource allocations to support system performance and availability. Virtual NAS Servers are mapped to specific **Storage Pools**, i.e., collections of storage nodes that are grouped together to simplify storage provisioning for specific applications or workgroups. Storage Pools contain one or more **files systems** that are used to store records.

- A file system intended to retain required records must be configured with the *Strict WORM File System* feature which hardens the files system and makes it capable of applying the most stringent retention protections to required records, in compliance with SEC Rules.
- Files and snapshots are stored in VSP One File and time-based[7] retention controls are applied as follows:
  - **Files** are transmitted via SMB, NFS, or FTP protocols and *Strict WORM* retention controls are explicitly applied by (a) transmitting an *atime* attribute set to a future date and (b) removing write permissions.
  - Point-in-time **snapshots** of entire file systems are captured manually by authorized administrators or automatically via pre-defined snapshot rules. Once created, the content of snapshots is immutable and cannot be modified or overwritten. *Snapshot* R*etention* controls are applied to prevent deletion, either automatically, via file system or rule defaults, or manually, during the snapshot process.

1.3.2 Assessment Scope

The scope of this assessment is focused specifically on the compliance-related capabilities of VSP One File, Release 15.1, when:

- Deployed on a VSP One File 32, 34 or38 gateway appliance with attached Hitachi premium storage arrays and
- Synchronous mirroring is enabled, which requires (a) an additional VSP One File gateway appliance, (b) Hitachi Disaster Recovery System license, and (c) a Global-Active Device license.

NOTES:

- VSP One File does not require the same software version on each node within a storage cluster. Care must be taken to assure that each storage node intended to retain required records is running the minimum specified VSP One File software version that supports WORM storage.
- VSP One File offers an alternative *non-Strict WORM File System* feature, which allows administrators to reformat or delete the file system, potentially deleting required records prematurely. This configuration has not been assessed for compliance with SEC Rules and is excluded from this assessment.
- Additionally, this assessment excludes:
  - The use of iSCSI or S3 protocols for storing files, since these protocols are not supported for use with the *Strict WORM File System* feature.
  - Integrations to public cloud storage such as Hitachi Cloud Platform, Microsoft Azure, or Amazon S3, since WORM retention controls set on VSP One File may not be applied to files migrated to cloud storage.

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

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

This section presents Cohasset's assessment of the functionality of Hitachi VSP One File, 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 VSP One File
- ***VSP One File 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 VSP One File, as described in Section 1.3, *VSP One File 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.*[8] [emphasis added]

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

> *[T]he audit-trail requirement applies to the final records required pursuant to the rules, rather than to drafts or iterations of records that would not otherwise be required to be maintained and preserved under Rules 17a-3 and 17a-4 or Rules 18a-5 and 18a-6.*[9] [emphasis added]

2.1.2 Compliance Assessment

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

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

2.2 Non-Rewriteable, Non-Erasable Record Format

2.2.1 Compliance Requirement

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

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

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

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

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

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

> *2019 interpretation further refined the 2003 interpretation. In particular, it noted that the 2003 interpretation described a process of integrated software and hardware codes and clarified that "a software solution that prevents the overwriting, erasing, or otherwise altering of a record during its required retention period would meet the requirements of the rule."*
> *****
> *In 2001, the Commission issued guidance that Rule 17a-4(f) was consistent with the ESIGN Act. The final amendments to Rule 17a-4(f) do not alter the rule in a way that would change this guidance.*[10] [emphasis added]

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

> *[A] broker-dealer must take appropriate steps to ensure that records are not deleted during periods when the regulatory retention period has lapsed but other legal requirements mandate that the records continue to be maintained, and the broker-dealer's storage system must allow records to be retained beyond the retentions periods specified in Commission rules.*[11] [emphasis added]

2.2.2 Compliance Assessment

It is Cohasset's opinion that the functionality of VSP One File, when configured and used with the *Strict WORM File System* and *Snapshot Retention* features, meets this SEC requirement to retain records in non-rewriteable, non-erasable format for the applied time-based[12] retention periods, when (a) properly configured, as described in Section 2.2.3 and (b) the considerations described in Section 2.2.4 are satisfied.

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

2.2.3 VSP One File Capabilities

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

2.2.3.1 Overview

- File systems that are intended to retain required records must be configured for use with the *Strict WORM File System* feature. Once this configuration is made, the file system cannot be reformatted or deleted by any means. The file system is capable of applying stringent retention controls to records, in compliance with SEC Rules 17a-4(f)(2) and 18a-6(e)(2).

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

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

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

- Files and snapshots are stored in VSP One File and time-based retention controls are applied as follows:
  - **Files** are transmitted via SMB, NFS, or FTP protocols and stored in virtual folders. *Strict WORM* retention controls are applied when the source system (a) transmits an atime attribute set to a future date and (b) write permissions are removed.
  - Point-in-time **snapshots** of entire file systems are captured manually by authorized administrators or automatically via pre-defined snapshot rules. By default, the content of a snapshot is immutable and cannot be modified or overwritten. Additionally, *Snapshot Retention* controls are applied to the snapshot to prevent deletion.
- The following table summarizes the retention controls that are applied at the underlying file system level are designed to preserve electronic records in a non-rewriteable, non-erasable format for the required retention period. See the subsections following this *Overview*, for detailed information on configuring the retention features and the resulting integrated controls.

	***Strict WORM* (Files)**	***Snapshot Retention* (Snapshots)**
Protecting record content and immutable attributes	• All write permissions are disabled for the stored content of the record and associated immutable attributes, thus protecting it against modification or overwrite for its lifespan. • A record cannot be renamed.	• By default, a snapshot and its associated system attributes are immutable and therefore protected against modifications or overwrites for its lifespan. • A snapshot may be renamed. Note: Rename operations are logged in the Management Audit Log.

Restricting changes to retention controls	• The *Strict WORM File System* feature, once configured for a file system, prohibits reformatting or deleting the file system and its contents.
	• The applied retention expiration date (atime) may be extended, but not reduced or removed.
	• See Section 2.2.3.3, *Record Definition and Controls.*
		• The *Strict WORM File System* feature, once configured for a file system, prohibits reformatting or deleting the file system.
		• The applied retention:
		  ○ May be extended by any user.
		  ○ May be reduced by administrators with special privileges, utilizing a time-bound password issued for a single target file system.
		Note: Procedural controls and monitoring are required to scrutinize privileged administrator actions taken to modify *Snapshot Retention* controls.

Applying and removing legal holds	• When a legal hold requires retention beyond the record's assigned retention period, retention must be extended. • See Section 2.2.3.4, *Legal Holds (Temporary Holds).*	
Restricting deletion of file system and records	• The record content and associated attributes cannot be deleted until the *atime* attribute value (retention expiration date) is in the past. • See Section 2.2.3.5, *Deletion Controls.*	• Snapshot content and associated attributes cannot be deleted by most users until the applied retention has expired. • Privileged administrators may override *Snapshot Retention* controls and therefore, may delete unexpired snapshots. Note: Procedural controls and monitoring are required to scrutinize privileged administrator actions taken to override *Snapshot Retention* controls.

2.2.3.2 VSP One File Configurations

- The following file system configurations are required to enable use of integrated *Strict WORM File System* and *Snapshot Retention* controls which are designed to preserve records in a non-rewriteable, non-erasable format for the applied retention period.

	File System Configurations
Strict WORM	● File systems that will store required records (files and snapshots) must be configured with the *Strict WORM File System* feature which: ○ Prohibits administrators from reformatting or deleting the file system. ○ Makes the file system **capable** of applying *Strict WORM* retention controls to retain files in a non-rewriteable, non-erasable format for the applied retention period. Note: *Strict WORM* retention controls can be applied to files only; not snapshots. ● Once Strict WORM has been configured for a file system, it cannot be changed to *non-Strict* or removed from the file system.
Snapshot Retention	● File systems that will store snapshots in compliance with SEC Rules must be configured to support *Snapshot Retention* by setting a default *Retention Interval* for the file system. ○ The default *Retention Interval* is automatically applied to each new snapshot's creation time to determine its retention, unless an explicit retention interval is provided by a snapshot rule or manual snapshot process. ○ The default *Retention Interval* is not applied to snapshots created internally by VSP One File's file system tools and other features such as replication.

2.2.3.3 Files - Record Definition and Applying *Strict WORM* Controls

- A file (i.e., record) is comprised of the following elements:
  - The **content** of the file.
  - **Immutable** system attributes, including a unique file name, creation timestamp, and unique identifier.
  - A **mutable** *atime* attribute (may be extended, not reduced).
- Files are not automatically locked with *Strict WORM* controls when stored in VSP One File. Rather, retention must be explicitly set for each record as follows:
  - The source system (a) transmits an *atime* attribute that is set to a future date and (b) removes write permissions for the file, or
  - The administrator utilizes the command line interface (CLI) to set the *atime* to a future date and remove write permissions for an existing file.
- The following table summarizes how retention controls are applied, based on the provided settings. Note: applied retention attributes are stored in the protected VSP One File onode (object node) for the record.

Write Permissions[13]	*Atime*	*Retention Expiration Date*
Removed	Future	The *atime* value is used as a retention expiration date and the file becomes immutable.
Allowed	Future	Record is stored with no retention controls.

[13] To remove write permissions when using SMB, the Boolean read-only attribute is set to Y(yes). With NFS, write permissions must be removed from the access control list (ACL).

Write Permissions[13]	*Atime*	*Retention Expiration Date*
Removed	Past	Record is stored with no retention controls.
Allowed	Past	Record is stored with no retention controls.

- *Atime* values greater than the year 2038 are not currently allowed. Note: An extension of this limit to the year 2106 (a 68-year extension) is planned for release 15.5.

2.2.3.4 Snapshots – Record Definition and Applying *Snapshot Retention* Controls

- Snapshots are space-efficient block level, point-in-time representations of complete file systems that can be taken at any desired interval, e.g., hourly, daily, weekly. The snapshot process only captures changes to data, i.e., blocks that have changed since the last snapshot.
- Up to 1,024 snapshots per file system can exist at any time. Options for creating snapshots include:
  - Automatically, via a configured snapshot rule which defines a schedule for when the snapshot process will run, e.g., hourly, daily, weekly. The resulting snapshots created by a rule are grouped together in an active queue.
    - If the active queue becomes full, a pre-defined Queue Full Policy is applied to resolve the issue. For compliance with SEC Rules, the default Queue Full Policy (*MoveOutOfQueueAndDelete*) must be configured, which assures that the oldest snapshot is removed from the active queue but **is not scheduled for deletion until its applied retention (if any) expires**.
  - Manually, by authorized administrators.

  Note: *Snapshot Retention* controls cannot be applied to snapshots created internally by VSP One File's file system tools and other similar features.
- A snapshot (i.e., a record) is comprised of the following elements:
  - The **content** of the snapshot.
  - **Immutable** attributes, including a unique ID and snapshot creation timestamp.
  - A **mutable** *Retention Interval* attribute (may be extended, not shortened) and a unique snapshot name. Note: For snapshots created manually, a unique name must be provided with the snapshot request. For snapshots created automatically via snapshot rules, a unique name is automatically assigned by VSP One File but may be changed.
- Once created, snapshots are immutable by default and cannot be modified or overwritten for their lifespan.
- A snapshot *Retention Interval* (maximum of 136 years, specified in terms of the number of seconds a snapshot is to be retained beyond its creation timestamp) is automatically applied during snapshot creation to prevent deletion, according to the following rules:
  - The default *Retention Interval* configured for the file system is applied to all newly created snapshots stored within that file system.

- A *Retention Interval* defined within a snapshot rule overrides the file system default and is applied to all new snapshots created by that rule.
- A *Retention Interval* specified during manual snapshot creation overrides both file system default and snapshot rule *Retention Intervals* and is applied to that one snapshot only.

2.2.3.5 Record Operations and Retention Controls

▶ The following table separately describes the integrated controls applied to files, when *Strict WORM* retention controls are applied, and to snapshots, when *Snapshot Retention* controls are applied.

	***Strict WORM* (Files)**	***Snapshot Retention* (Snapshots)**
Protecting record content and immutable attributes	• All write permissions are disabled for the stored content of the record and associated immutable attributes, thus protecting it against modification or overwrite for its lifespan. • A record cannot be renamed.	• By default, a snapshot and its associated system attributes are immutable and therefore protected against modifications or overwrites for its lifespan. • Snapshot restore operations are not permitted for a *Strict WORM File System.* • A snapshot may be renamed. Note: Rename operations are logged in the Management Audit Log.
Restricting changes to retention controls	• The *Strict WORM File System* feature, once configured for a file system, prohibits reformatting or deleting the file system and its contents by any user. • The applied retention may be extended, but not reduced or removed. • See Section 2.2.3.3, *Record Definition and Controls.*	• The *Strict WORM File System* feature, once configured for a file system, prohibits reformatting or deleting the file system by any user. • The applied retention: ○ May be extended by any user. ○ May be reduced by administrators with special privileges, utilizing a time-bound password issued for a single target file system. Note: Procedural controls and monitoring are required to scrutinize privileged administrator actions taken to modify *Snapshot Retention* controls.
Applying and removing legal holds	• When a legal hold requires retention beyond the record's assigned retention period, retention must be extended. • See Section 2.2.3.4, *Legal Holds (Temporary Holds).*	
Restricting deletion of file system and records	• The record content and associated attributes cannot be deleted until the *atime* attribute value is in the past. • See Section 2.2.3.5, *Deletion Controls.*	• Snapshot content and associated attributes cannot be deleted by most users until the applied retention has expired. • Privileged administrators may override *Snapshot Retention* controls and therefore, may delete unexpired snapshots. Note: Procedural controls and monitoring are required to scrutinize privileged administrator actions taken to override *Snapshot Retention* controls. • Additionally, when the active snapshot queue size is exceeded: ○ When the *MoveOutOfQueueAndDelete* Queue Full Policy is configured, snapshot retention is honored.

	***Strict WORM* (Files)**	***Snapshot Retention* (Snapshots)**
		○ Otherwise, the oldest snapshot may be prematurely deleted by an *IgnoreRetentionAndDelete* Queue Full Policy. ○ Accordingly, policies and monitoring must be established for the proper configuration of snapshot rules to ensure that snapshot retention controls are not bypassed. ● See Section 2.2.3.5, *Deletion Controls*.
Copying records	● A record may be copied within the same file system: ○ If copied via NFS protocol, the target file is locked and the retention is set to 2038 (max allowed). Note: An extension of this limit to the year 2106 (a 68-year extension) is planned for release 15.5. ○ If copied via SMB protocol or Linux cp command, the source *atime* is not preserved and therefore, the target file is not locked. ● A record may be copied to a different file system. Source file retention controls are not copied to the target file.	● Snapshots may not be copied.
Moving records	● Move operations are not supported.	

2.2.3.6 Legal Holds (Temporary Holds)

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

► When a legal hold requires retention of a record beyond its currently assigned retention period, retention must be extended. Multiple extensions may be required to assure retention for the duration of the hold.

2.2.3.7 Deletion Controls

► The following table summarizes actions taken to delete records and associated attributes protected by *Strict WORM* and *Snapshot Retention* controls.

	***Strict WORM* (Files)**	***Snapshot Retention* (Snapshots)**
Deletion eligibility	● Files are eligible for deletion when the applied *atime* value is in the past.	● Snapshots are eligible for deletion when the dynamically calculated retention period (the applied *Retention Interval* added to the snapshot creation timestamp) has expired.
Deleting a record	● **Eligible** records are not automatically deleted.	● **Eligible** snapshots that were created via a snapshot rule are automatically deleted**. Eligible** snapshots that were manually created are not automatically deleted. ○ Automatic deletion of snapshots is prohibited if system time is considered inaccurate. See Section 2.2.3.9, *Clock Management*.

	***Strict WORM* (Files)**	***Snapshot Retention* (Snapshots)**
		• Privileged administrators may override *Snapshot Retention* controls and therefore, may delete unexpired snapshots. Note: Procedural controls and monitoring are required to scrutinize privileged administrator actions taken to override *Snapshot Retention* controls.
Deleting file systems	• File systems configured with the *Strict WORM File System* feature cannot be deleted.	

2.2.3.8 Security

In addition to the stringent retention protection and management controls described above, VSP One File provides the following security capabilities, which support the authenticity and reliability of the records:

- VSP One File provides the following encryption capabilities to protect data in transit:
  - SMB 3.0 uses the AES128 CCM encryption algorithm. Outgoing SMB2/SMB3 messages are signed using HMAC-SH256 or AES-128-CMAC respectively. All encryption keys for in-transit data encryption are session-based.
  - NFS supports RPCSEC_GSS style of security with Kerberos. NFS exports can be configured to enforce this, including requiring that requests be signed and/or encrypted.
    - For Kerberos, AES256-CTS-HMAC-SHA1-96 and AES128-CTS-HMAC-SHA1-96 are supported.
    - For NFSv4.1 SP4_MACH_CRED is supported, meaning a client's server-side state can be changed only if the request is signed (or encrypted) by the client's machine credential.
- VSP One File provides encryption capabilities for data at rest on Hitachi premium storage arrays (VSP One Block).
  - Hitachi VSP One Block provides a license based "data encryption at rest" capability. This can be a hardware or CPU-based implementation which uses AES256 encryption and an internal KMS.

2.2.3.9 Clock Management

- To meet this requirement of the Rules, Hitachi recommends that every VSP One File system clock be synchronized to an external Network Time Protocol (NTP) clock. Continued synchronization assures that timestamps are accurate when records are fully written and help protect against premature deletion of records.
- Specific to snapshots (though not relevant to files), the *Time Protection* feature protects against inadvertent or malicious reconfiguration of system time and NTP synchronization settings by any user or administrator.
  - System time is verified on boot and monitored regularly. If time deviates outside of an allowable range, a severe event is written to the Event Log and system time is considered inaccurate. Note: while system time is flagged as inaccurate, deletion of eligible *snapshots* is prohibited, however, *files* that are past their applied retention may be deleted. **Procedural controls and monitoring are required to scrutinize the automated deletion of files past their applied retention, while system time is considered inaccurate**.

- System time must be reset by an authorized administrator using a system-specific, time-sensitive token obtained from Hitachi. After reset, normal time monitoring processes resume.

2.2.4 Additional Considerations

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

- Configuring any file system that may be utilized to store SEC-regulated books and records with the *Strict WORM File System* feature. Furthermore, configuring an appropriate default *Retention Interval* to assure compliant retention of snapshots.
- Configuring snapshot rules with Queue Full Policies set to *MoveOutOfQueueAndDelete*, which honors applied retention when snapshot queue size is exceeded.
- Ensuring appropriate retention controls are set for all required records by (a) explicitly transmitting them for files or (b) setting appropriate snapshot rule *Retention Intervals* for snapshots, if retention requirements differ from the file system default.
- Extending retention as necessary to meet legal hold preservation requirements; multiple extensions may be required to ensure records are preserved for the duration of the legal hold.
- Storing records requiring event-based[14] retention periods in a separate compliant system or otherwise planning for event-based retention, since VSP One File does not currently support event-based retention periods.
- Implementing procedural controls and monitoring to scrutinize administrator actions related to overriding *Snapshot Retention* controls.
- Implementing procedural controls and monitoring to scrutinize the automated deletion of files past their applied retention, while VSP One File system time is considered inaccurate.

Additionally, the regulated entity is responsible for (a) authorizing user privileges and (b) maintaining appropriate technology, encryption keys, and other information and services needed to retain the records.

2.3 Record Storage Verification

2.3.1 Compliance Requirement

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

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

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

[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 VSP One File 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 VSP One File Capabilities

The recording and post-recording verification processes of VSP One File are described below.

2.3.3.1 Recording Process

- VSP One File gateways, attached to Hitachi VSP One Block storage arrays, support the 100% Data Availability Guarantee. Terms and conditions apply; please see the 100% data availability guarantee.
  - Stable storage is facilitated via NVRAM (Non-Volatile Random Access Memory), where data is protected in flight until a successful write to disk is verified.
  - File systems are resilient with multiple mechanisms designed to protect data, including (a) cyclical redundancy checks (CRC's) to protect metadata mappings of all file blocks, (b) RAID 6 protection of all data blocks, and (c) file system level checkpoints which keep track of file system health and allow for rollback recovery when necessary.

2.3.3.2 Post-Recording Verification Process

- During read back of records, disk error detection and correction are applied to correct any in-error data on the storage disk. Should automatic correction be unsuccessful, the records must be recovered from a duplicate copy.

2.3.4 Additional Considerations

- The source system is responsible for transmitting the complete contents of the required records and VSP One File 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 VSP One File meets this SEC requirement to maintain capacity to readily download and transfer the records and information used to locate the records, when the considerations described in Section 2.4.4 are satisfied.

2.4.3 VSP One File Capabilities

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

- Each record in VSP One File is assigned a unique identifier, which facilitates findability. Specifically, VSP One File captures the following metadata for each record and immutably retains this metadata for the lifespan of the record.

	Files	Snapshots
Unique identifier	• A unique name is transmitted and stored with every file and cannot be modified by any user or mechanism for its lifespan.	• A unique ID is assigned to each snapshot and cannot be modified by any user or mechanism for its lifespan.
Creation Timestamp	• The system generates a creation timestamp for each record as it is stored in VSP One File which cannot be modified by any user or other mechanism.	• The system generates a creation timestamp for each snapshot at the completion of the snapshot process which cannot be modified by any user or other mechanism.

- VSP One File gateway appliances with attached Hitachi premium storage arrays, support block level file storage with a 100% data availability guarantee.
- File share directories and contents may be manually navigated via standard CLI commands or third-party search tools.
- Using NFS or SMB file storage protocols, the source system can request one or more specific records to be accessed, reproduced, and transferred to a medium acceptable under the Rule.
- Lists of snapshots and associated attributes can be produced via CLI commands or programmatically via APIs.

2.4.4 Additional Considerations

Additionally, the regulated entity is responsible for (a) authorizing user privileges, (b) maintaining appropriate technology and resource capacity, encryption keys, and other information and services needed to use VSP One File 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 VSP One File meets paragraphs (A) of this SEC requirement by retaining a persistent duplicate copy of the records, when (a) properly configured with Hitachi Disaster Recovery System (HDRS) in conjunction with Global-Active Device (GAD) metro clustering, as described in Section 2.5.3 and (b) the considerations described in Section 2.5.4 are satisfied.

2.5.3 VSP One File Capabilities

The option for meeting the record redundancy requirement is described below.

2.5.3.1 Redundant Set of Records

- The Hitachi Disaster Recovery System (HDRS) in conjunction with Global-Active Device (GAD) metro clustering provides dual-site, fully synchronous active-active clustering.

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

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

- For files, a duplicate copy is created by mirroring data from the source to a target system, with updates made to both sites:
  - Write operations are not considered successful until mirroring is complete.
  - Failover from one site to the other is completely automatic, meaning source systems access replicated data from whichever site has the shortest path.
- GAD ensures that the entire file system is mirrored at the storage layer. Thus, both the source and target locations have a complete copy of the filesystem, including both files and snapshots. Note: A snapshot is not a duplicate copy of an entire file system, but rather, an entry-point reference map to data within that file system.

2.5.4 Additional Considerations

Additionally, the regulated entity is responsible for maintaining the technology, storage capacity, encryption keys, and other information and services needed to use VSP One File and permit access to the redundant records.

2.6 Audit System

2.6.1 Compliance Requirement

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

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

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

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

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

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

2.6.2 Compliance Assessment

Cohasset asserts that VSP One File supports the regulated entity's efforts to meet this SEC requirement for an audit system.

2.6.3 VSP One File Capabilities

The regulated entity is responsible for an audit system, and compliance is supported by VSP One File.

- For each record stored, VSP One File retains the following audit information.

	Files	Snapshots
Unique identifier	• A unique name is transmitted and stored with every file and cannot be modified by any user or mechanism for its lifespan.	• A unique ID is assigned to each snapshot and cannot be modified by any user or mechanism for its lifespan.
Creation Timestamp	• The system generates a creation timestamp for each record as it is stored in VSP One File which cannot be modified by any user or other mechanism.	• The system generates a creation timestamp for each snapshot at the completion of the snapshot process which cannot be modified by any user or other mechanism.

These attributes are *immutably* stored for the lifespan of the record.

- Records are immutable, meaning changes are disallowed; therefore, tracking of the inputting of changes made is not relevant to VSP One File.
- In addition to the immutable records and associated attributes, VSP One File provides the following snapshot and system time audit capabilities:
  - The **Management Audit Log** captures events related to snapshots, including:
    - Creation or modification of snapshot rules,
    - Snapshot creation,
    - Extending the Retention Interval for a snapshot,
    - Changing a snapshot name,
    - Snapshot deletion.

    Events are retained in the Management Audit Log file indefinitely and may not be modified or cleared by any user or mechanism. Additionally, log events may be read by an external log server.
  - The **Event Log** captures warnings related to system time. Should the system time be modified and considered inaccurate, VSP One File issues a severe warning event which is captured within the log.
    - Events are retained in the Event Log file indefinitely and may only be cleared by a user with dev-level privileges.

2.6.4 Additional Considerations

The regulated entity is responsible for maintaining an audit system for inputting records and changes made to the records (though VSP One File disallows changes to stored files and snapshots). In addition to relying on the immutable metadata, the regulated entity may utilize VSP One File audit features alone or in conjunction with another system.

In addition, the regulated entity is responsible for: (a) authorizing user privileges and (b) providing requested information to the regulator, in the requested format.

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

This section contains a summary assessment of the functionality of Hitachi Vantara's VSP One File, as described in Section 1.3, *VSP One File 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 VSP One File with the:

- *Strict WORM File System* feature, which provides both overwrite protection and strict deletion and retention protections for files and
- *Snapshot Retention* feature, which is a less-restrictive feature that provides overwrite protections but requires administrative procedures and monitoring to ensure compliant retention, since administrators are allowed to override retention protections.

In the following table, Cohasset correlates specific *principles-based* CFTC requirements for electronic records with the assessed functionality of VSP One File. The first column enumerates the CFTC regulation. The second column provides Cohasset's analysis and opinion regarding the ability of VSP One File, relative to these requirements.

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

CFTC 1.31(c)-(d) Regulation [emphasis added]	**Compliance Assessment Relative to CFTC 1.31(c)-(d)**
(c) Form and manner of retention. Unless specified elsewhere in the Act or Commission regulations in this chapter, all regulatory records must be created and retained by a records entity in accordance with the following requirements: *(1) Generally. Each records entity shall retain regulatory records in a form and manner that ensures the authenticity and reliability of such regulatory records in accordance with the Act and Commission regulations in this chapter.* *(2) Electronic regulatory records. Each records entity maintaining electronic regulatory records shall establish appropriate systems and controls that ensure the authenticity and reliability of electronic regulatory records, including, without limitation:* *(i) Systems that maintain the security, signature, and data as necessary to ensure the authenticity of the information contained in electronic regulatory records and to monitor compliance with the Act and Commission regulations in this chapter;*	It is Cohasset's opinion that the CFTC requirements in (c)(1) and (c)(2)(i), for records[18] with time-based retention periods, are met by the functionality of VSP One File, with the *Strict WORM File System* and *Snapshot Retention* features. The functionality that supports retention, authenticity and reliability of electronic records is described in the following sections of this report: ● Section 2.2, *Non-Rewriteable, Non-Erasable Record Format* ● Section 2.3, *Record Storage Verification* ● Section 2.4, *Capacity to Download and Transfer Records and Location Information* ● Section 2.6, *Audit System* Additionally, for *records stored electronically*, the CFTC definition of *regulatory records* in 17 CFR § 1.31(a) includes information to access, search and display records, as well as data on records creation, formatting and modification: *Regulatory records means all books and records required to be kept by the Act or Commission regulations in this chapter, including any record of any correction or other amendment to such books and records, provided that, with respect to such books and records stored electronically, regulatory records shall also include:* *(i) Any data necessary to access, search, or display any such books and records; and* *(ii) All data produced and stored electronically describing how and when such books and records were created, formatted, or modified.* [emphasis added] VSP One File retains immutable attributes (e.g., unique file name or snapshot ID and creation timestamp) as an integral component of the records, and, therefore, these attributes are subject to the same retention controls as the associated record. These immutable attributes support both (a) records access, search and display and (b) audit system and accountability for inputting the records. Additionally, a retention attribute is stored as a mutable attribute for each record. The most recent value of the retention attribute is retained for the same time period as the associated records. Further, VSP One File in conjunction with the Management Audit Log tracks audit events and retains the events indefinitely. For additional information, see Section 2.6, *Audit System*.
(ii) Systems that ensure the records entity is able to produce electronic regulatory records in accordance with this section, and ensure the availability of such regulatory records in the event of an emergency or other disruption of the records entity's electronic record retention systems; and	It is Cohasset's opinion that VSP One File capabilities described in Section 2.5, *Record Redundancy*, including a method for a persistent duplicate copy to reestablish the records and associated system metadata, meet the CFTC requirements (c)(2)(ii) to *ensure the availability of such regulatory records in the event of an emergency or other disruption of the records entity's electronic record retention systems*.

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

CFTC 1.31(c)-(d) Regulation [emphasis added]	**Compliance Assessment Relative to CFTC 1.31(c)-(d)**
(iii) The creation and maintenance of an up-to-date inventory that identifies and describes each system that maintains information necessary for accessing or producing electronic regulatory records.	The regulated entity is required to create and retain an *up-to-date inventory*, as required for compliance with 17 CFR § 1.31(c)(iii).
(d) Inspection and production of regulatory records. Unless specified elsewhere in the Act or Commission regulations in this chapter, a records entity, at its own expense, must produce or make accessible for inspection all regulatory records in accordance with the following requirements: *(1) Inspection. All regulatory records shall be open to inspection by any representative of the Commission or the United States Department of Justice.* *(2) Production of **paper** regulatory records. **** *(3) Production of **electronic** regulatory records.* *(i) A request from a Commission representative for electronic regulatory records will specify a reasonable form and medium in which a records entity must produce such regulatory records.* *(ii) A records entity must produce such regulatory records in the form and medium requested promptly, upon request, unless otherwise directed by the Commission representative.* *(4) Production of **original** regulatory records. ****	It is Cohasset's opinion that VSP One File has features that support the regulated entity's efforts to comply with requests for inspection and production of records, as described in. ● Section 2.2, *Non-Rewriteable, Non-Erasable Record Format* ● Section 2.4, *Capacity to Download and Transfer Records and Location Information* ● Section 2.6, *Audit System*

4 • Summary Assessment of Compliance with MiFID II Delegated Regulation(72)(1)

The objective of this section is to document Cohasset's assessment of the functionality of VSP One File, as described in Section 1.3, *VSP One File Overview and Assessment Scope*, in comparison to the following requirements of the *Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing MiFID II (the MiFID II Delegated Regulation).* Specifically, Article 72(1) defines medium and retention of records requirements:

> *1. The records shall be retained in a medium that allows the storage of information in a way accessible for future reference by the competent authority, and in such a form and manner that the following conditions are met:*
> *(a) the competent authority is able to access them readily and to reconstitute each key stage of the processing of each transaction;*
> *(b) it is possible for any corrections or other amendments, and the contents of the records prior to such corrections or amendments, to be easily ascertained;*
> *(c) it is not possible for the records otherwise to be manipulated or altered;*
> *(d) it allows IT or any other efficient exploitation when the analysis of the data cannot be easily carried out due to the volume and the nature of the data; and*
> *(e) the firm's arrangements comply with the record keeping requirements irrespective of the technology used.* [emphasis added]

Paragraph (e), above, recognizes the technology evolution and defines requirements or conditions for regulated entities that retain records electronically. The approach is consistent with the SEC, which also sets forth standards that the electronic storage media must satisfy to be acceptable.

Additionally, Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments (MiFID II) defines durable medium as follows:

> *(62) 'durable medium' means any instrument which:*
> *(a) enables a client to store information addressed personally to that client in a way accessible for future reference and for a period of time adequate for the purposes of the information; and*
> *(b) allows the unchanged reproduction of the information stored;* [emphasis added*]*

While the above pertains to enabling the client to store and access its information, regulated entities often apply the MiFID II durable medium requirements to internally retained information, assuring it is immutable, retained for the appropriate time period and stored in a manner that assures unchanged reproduction. For this reason, Cohasset included this citation in its analysis for this section of the report.

In Section 2 of this report, Cohasset assesses VSP One File with the:

- *Strict WORM File System* feature, which provides both overwrite protection and strict deletion and retention protections for files and

- *Snapshot Retention* feature, which is a less-restrictive feature that provides overwrite protections but requires administrative procedures and monitoring to ensure compliant retention, since administrators are allowed to override retention protections.

In the following table, Cohasset correlates specific MiFID II requirements for electronic records with the functionality of VSP One File when configured to meet SEC requirements. The first column enumerates specific electronic records requirements for (a) *durable medium* in MiFID II and (b) the *medium* and retention of records in the *Delegated Regulation,* which supplements MiFID II. The second column provides Cohasset's analysis and opinion regarding the ability of VSP One File, relative to these requirements.

Regulatory excerpts of MiFID II media requirements [emphasis added]	**Compliance assessment and analysis of VSP One File relative to these MiFID II media requirements**
Directive 2014/65/EU (MiFID II) Article 4(1)(62) *(62) 'durable medium' means any instrument which:* *(a) enables a client to store information addressed personally to that client in a way accessible for future reference and for a period of time adequate for the purposes of the information* ***** **Commission Delegated Regulation (EU) 2017/565, (the MiFID II Delegated Regulation), Article 72(1)** *(1) The records shall be retained in a medium that allows the storage of information in a way accessible for future reference by the competent authority, and in such a form and manner that the following conditions are met:* *****	While these requirements pertain to the regulated entity's client and regulator, the regulated entity itself would have a similar need to store the record for the required retention period. It is Cohasset's opinion that the following VSP One File features apply time-based retention controls to records and associated system attributes: ● *Strict WORM File System* feature and ● *Snapshot Retention* feature. See Section 2.2, *Non-Rewriteable, Non-Erasable Record Format*, for additional information. Further, VSP One File assures the accurate recording (storage) of the record content and associated attributes, as explained in Section 2.3, *Record Storage Verification*. The quality and accuracy of the recording process is verified: (a) during the initial recording of the record and (b) using post-recording verification during read-back.
Directive 2014/65/EU (MiFID II) Article 4(1)(62) *(62) 'durable medium' means any instrument which:* ***** *(b) allows the unchanged reproduction of the information stored;* **Commission Delegated Regulation (EU) 2017/565, (the MiFID II Delegated Regulation), Article 72(1)** *1. The records shall be retained in a medium that allows the storage of information in a way accessible for future reference by the competent authority, and in such a form and manner that the following conditions are met:* ***** *(b) it is possible for any corrections or other amendments, and the contents of the records prior to such corrections or amendments, to be easily ascertained;* *(c) it is not possible for the records otherwise to be manipulated or altered;* *****	It is Cohasset's opinion that the assessed features of VSP One File, achieve the non-rewriteable, non-erasable storage requirements necessary to assure that record content is unchangeable. See Section 2.2, *Non-Rewriteable, Non-Erasable Record Format*, for additional information. If the regulated entity corrects or amends a record in the source system, it must store the new rendition as a new record. The features for non-rewriteable, non-erasable format assure that the original record is not modified.

Regulatory excerpts of MiFID II media requirements [emphasis added]	**Compliance assessment and analysis of VSP One File relative to these MiFID II media requirements**
Directive 2014/65/EU (MiFID II) Article 4(1)(62) *(62) 'durable medium' means any instrument which:* *(a) enables a client to store information addressed personally to that client in a way accessible for future reference and for a period of time adequate for the purposes of the information* *(b) allows the unchanged reproduction of the information stored;* **Commission Delegated Regulation (EU) 2017/565, (the MiFID II Delegated Regulation), Article 72(1)** *1. The records shall be retained in a medium that allows the storage of information in a way accessible for future reference by the competent authority, and in such a form and manner that the following conditions are met:* ***** *(a) the competent authority is able to access them readily and to reconstitute each key stage of the processing of each transaction;* ***** *(d) it allows IT or any other efficient exploitation when the analysis of the data cannot be easily carried out due to the volume and the nature of the data; and* *****	Cohasset asserts that VSP One File provides the following tools for retrieving records: ● File share directories and contents may be manually navigated via standard CLI commands or 3rd party search tools. ● Using NFS or SMB file storage protocols, the source system can request one or more specific records to be downloaded for viewing, reproduction, or transfer to a medium acceptable under the Rule. ● Lists of snapshots and associated attributes can be produced via CLI commands or programmatically via APIs. See Section 2.4, *Capacity to Download and Transfer Records and Location Information*, for additional information. Further, when HDRS and GAD services are properly configured, records and associated attributes are synchronously mirrored which ensures that records are readily available. See Section 2.5, *Record Redundancy*, for additional information.
Directive 2014/65/EU (MiFID II) Article 4(1)(62) *N/A* **Commission Delegated Regulation (EU) 2017/565, (the MiFID II Delegated Regulation), Article 72(1)** *1. The records shall be retained in a medium that allows the storage of information in a way accessible for future reference by the competent authority, and in such a form and manner that the following conditions are met:* ***** *(e) the firm's arrangements comply with the record keeping requirements irrespective of the technology used.* *****	Cohasset asserts that VSP One File provides the following tools for retrieving records: ● File share directories and contents may be manually navigated via standard CLI commands or 3rd party search tools. ● Using NFS or SMB file storage protocols, the source system can request one or more specific records to be downloaded for viewing, reproduction, or transfer to a medium acceptable under the Rule. ● Lists of snapshots and associated attributes can be produced via CLI commands or programmatically via APIs. See Section 2.4, *Capacity to Download and Transfer Records and Location Information*, for additional information. As may be required, the regulated entity may transfer records to other media or migrate records to new file formats, in advance of technological obsolescence.

5 • Conclusions

Cohasset assessed the functionality of VSP One File[19] in comparison to the electronic recordkeeping system requirements set forth in SEC Rules 17a-4(f)(2) and 18a-6(e)(2) and described audit system features that support the regulated entity as it meets the requirements of SEC Rules 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii).

Cohasset determined that VSP One File, when properly configured, has the following functionality, which meets the regulatory requirements:

- Maintains records and immutable system attributes in a non-rewriteable, non-erasable format for (a) time-based retention periods, using the *Strict WORM File System* and *Snapshot Retention* features.
- Allows extending retention on records to immutably preserve records for a subpoena, legal hold or similar circumstances.
- Prohibits deletion of a record and its immutable metadata until the retention period for the record is expired. Note: When the less-restrictive *Snapshot Retention* feature is applied to snapshots, procedural controls and monitoring are required to scrutinize administrator actions to override retention controls or prematurely delete required records.
- Verifies the accuracy of the process for storing and retaining the records using a combination of checks and balances inherent in the VSP One File advanced storage technology.
- Provides the capacity and tools to (a) search for records, (b) list the records, and (c) download and/or restore the records and associated system attributes for a local tool to render as a human-readable view and produce in the requested electronic format.
- Maintains redundancy to retrieve an accurate replica of the record 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 VSP One File, when properly configured and the additional considerations are satisfied, meets the electronic recordkeeping system requirements of SEC Rules 17a-4(f)(2) and 18a-6(e)(2) and FINRA Rule 4511(c), as well as supports the regulated entity in its compliance with the audit system requirements in SEC Rules 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii). In addition, the assessed capabilities meet the principles-based electronic records requirements of CFTC Rule 1.31(c)-(d) and the *medium and retention of records* requirements of the *MiFID II Delegated Regulation(72)(1)*.

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

Appendix A • Overview of Relevant Electronic Records Requirements

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

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

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

Effective January 3, 2023, the U.S. Securities and Exchange Commission (SEC) promulgated amendments[20] to 17 CFR § 240.17a-4 (Rule 17a-4) and 17 CFR § 240.18a-6 (Rule 18a-6), which define more technology-neutral requirements for electronic recordkeeping systems.

> *The objective is to prescribe rules that remain workable as record maintenance and preservation technologies evolve over time but also to set forth requirements designed to ensure that broker-dealers and SBS Entities maintain and preserve records in a manner that promotes their integrity, authenticity, and accessibility.*[21] [emphasis added]

These 2022 amendments (a) provide a record 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 SBSD/MSBSP Recordkeeping Adopting Release).

---

23 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.
24 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.
25 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66418.
26 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66419.

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

> *A broker-dealer would not violate the requirement in paragraph* [(f)(2)(i)(B) (refreshed citation number)] *of the rule if it used an electronic storage system that prevents the overwriting, erasing or otherwise altering of a record during its required retention period through the use of integrated hardware and software control codes.*[27] [emphasis added]

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

> *The Commission is clarifying that a software solution that prevents the overwriting, erasing, or otherwise altering of a record during its required retention period would meet the requirements of the rule.*[28] [emphasis added]

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

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

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

> *[A] broker-dealer must take appropriate steps to ensure that records are not deleted during periods when the regulatory retention period has lapsed but other legal requirements mandate that the records continue to be maintained, and the broker-dealer's storage system must allow records to be retained beyond the retentions periods specified in Commission rules.*[29] [emphasis added]

See Section 2, *Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e),* for each SEC electronic recordkeeping system requirement and a description of the functionality of VSP One File 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 Interpretative Release, 68 FR 25282.

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

29 2003 Interpretative Release, 68 FR 25283.

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

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 VSP One File 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).

A.4 Overview of the *Medium* and *Retention of Records* Requirements of MiFID II

Markets in Financial Instruments Directive II (MiFID II), approved by the European Parliament as *Directive 2014/65/EU,* became effective January 3, 2018. Specifically, Article 4(1)(62) of MiFID II defines durable medium as:

> *(62) 'durable medium' means any instrument which:*
> *(a) enables a client to store information addressed personally to that client in a way accessible for future reference and for a period of time adequate for the purposes of the information; and*
> *(b) allows the unchanged reproduction of the information stored;* [emphasis added]

While the above pertains to enabling the client to store and access its information, regulated entities often apply the MiFID II durable medium requirements to internally retained information, assuring it is immutable, retained for the appropriate time period and stored in a manner that assures the unchanged reproduction.

Further, with implementation of the revised MiFID II, investment firms must arrange for records to be kept for all services, activities and transactions. The key recordkeeping provisions are in Article 16, *Organisational requirements*, paragraphs 6 and 7:

> ***6.*** *An investment firm shall arrange for records to be kept of all services, activities and transactions undertaken by it which shall be sufficient to enable the competent authority to fulfil its supervisory tasks and to perform the enforcement actions under this Directive, Regulation (EU) No 600/2014, Directive 2014/57/EU and Regulation (EU) No 596/2014, and in particular to ascertain that the investment firm has complied with all obligations including those with respect to clients or potential clients and to the integrity of the market.*
> ***7.*** *Records shall include the recording of telephone conversations or electronic communications relating to, at least, transactions concluded when dealing on own account and the provision of client order services that relate to the reception, transmission and execution of client orders.*
> *Such telephone conversations and electronic communications shall also include those that are intended to result in transactions concluded when dealing on own account or in the provision of client order services that relate to the reception, transmission and execution of client orders, even if those conversations or communications do not result in the conclusion of such transactions or in the provision of client order services.*
> *For those purposes, an investment firm shall take all reasonable steps to record relevant telephone conversations and electronic communications, made with, sent from or received by equipment provided by the investment firm to an employee or contractor or the use of which by an employee or contractor has been accepted or permitted by the investment firm.*
> *****
> *Orders may be placed by clients through other channels, however such communications must be made in a durable medium such as mails, faxes, emails or documentation of client orders made at meetings. In particular, the content of relevant face-to-face conversations with a client may be recorded by using written minutes or notes. Such orders shall be considered equivalent to orders received by telephone.*
> *****
> *The records kept in accordance with this paragraph shall be provided to the client involved upon request and shall be kept for a period of five years and, where requested by the competent authority, for a period of up to seven years.* [emphasis added]

Article 16(6) allowed the Commission to make delegated legislation, resulting in the issuance of *Commission Delegated Regulation (EU) 2017/565* (*the MiFID II Delegated Regulation*).

The *MiFID II Delegated Regulation* in Section 8, *Record-keeping*, Article 72, *Retention of records*, paragraph 1, specifies:

> *1. The records shall be retained in a medium that allows the storage of information in a way accessible for future reference by the competent authority, and in such a form and manner that the following conditions are met:*
>
> *(a) the competent authority is able to access them readily and to reconstitute each key stage of the processing of each transaction;*
>
> *(b) it is possible for any corrections or other amendments, and the contents of the records prior to such corrections or amendments, to be easily ascertained;*
>
> *(c) it is not possible for the records otherwise to be manipulated or altered;*
>
> *(d) it allows IT or any other efficient exploitation when the analysis of the data cannot be easily carried out due to the volume and the nature of the data; and*
>
> *(e) the firm's arrangements comply with the record keeping requirements irrespective of the technology used.* [emphasis added]

See Section 4, *Summary Assessment of Compliance with the MiFID II Delegated Regulation(72)(1),* for a summary assessment of the capabilities of VSP One File in relation to requirements for (a) *durable medium* in MiFID II and (b) medium and retention of records in the *MiFID II Delegated Regulation*.

About Cohasset Associates, Inc.

Cohasset Associates, Inc. (www.cohasset.com) is a professional consulting firm, specializing in records management and information governance. Drawing on more than fifty years of experience, Cohasset provides its clients with innovative advice on managing their electronic information as the digital age creates operational paradigms, complex technical challenges and unprecedented legal issues.

Cohasset provides award-winning professional services in four areas: management consulting, education, thought-leadership and legal research.

Management Consulting: Cohasset strategizes with its multi-national and domestic clients, designing and supporting implementations that promote interdisciplinary information governance, achieve business objectives, optimize information value, improve compliance, and mitigate information-related risk.

Cohasset is described as *the only management consulting firm in its field with its feet in the trenches and its eye on the horizon*. This fusion of practical experience and vision, combined with a commitment to excellence, results in Cohasset's extraordinary record of accomplishments.

Education: Cohasset is distinguished through its delivery of exceptional and timely education and training on records and information lifecycle management and information governance.

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

For domestic and international clients, Cohasset:

- *Formulates information governance implementation strategies*
- *Develops policies and standards for records management and information governance*
- *Creates clear and streamlined retention schedules*
- *Prepares training and communications for executives, the RIM network and all employees*
- *Leverages content analytics to improve lifecycle controls for large volumes of eligible information, enabling clients to classify information, separate high-value information and delete what has expired*
- *Designs and supports the implementation of information lifecycle practices that mitigate the cost and risk associated with over-retention*
- *Defines strategy and design for information governance in collaboration tools, such as M365*
- *Defines technical and functional requirements and assists with the deployment of enterprise content management and collaboration tools*

Legal Research: Cohasset is nationally respected for its direction on information governance legal issues – from retention schedules to compliance with the regulatory requirements associated with the use of electronic or digital storage media.