Cohasset Associates

Pure Storage® FlashBlade™ File Storage

COMPLIANCE ASSESSMENT

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

Abstract

Pure Storage® FlashBlade™ is a highly-scalable all-flash integrated storage solution. FlashBlade combines both file and object storage. This report assesses only FlashBlade File Storage. Pure Storage designed the WORM features and other compliance capabilities to meet securities industry requirements for preserving records in non-rewriteable, non-erasable format for the applied retention period and legal holds.

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

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

It is Cohasset's opinion that FlashBlade File Storage, when the WORM features and other compliance capabilities are properly configured and applied, has functionality that meets the electronic recordkeeping system requirements of SEC Rules 17a-4(f)(2) and 18a-6(e)(2) and FINRA Rule 4511(c), as well as supports the regulated entity in its compliance with SEC Rules 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii). Additionally, the assessed functionality of FlashBlade File Storage meets the principles-based requirements of CFTC Rule 1.31(c)-(d).

COHASSET'S INDUSTRY INSIGHT AND EXPERIENCE

Core to our practice is the delivery of records management and information governance professional consulting services, and education and training. Cohasset's expert consulting services support regulated organizations, including those in financial services. Cohasset serves both domestic and multi-national clients, aligning information lifecycle controls to their organizations' business priorities, facilitating regulatory compliance and risk mitigation, while generating quantifiable business efficiency.

Cohasset assesses a range of electronic recordkeeping systems, each designed to meet the requirements of the Securities and Exchange Commission Rules 17a-4(f)(2) and 18a-6(e)(2) for record audit-trail and non-rewriteable, non-erasable record formats, considering the SEC 2001, 2003 and 2019 interpretations. For the non-rewriteable, non-erasable record, these interpretations authorize the use of erasable storage, conditioned on integrated software or hardware control codes, to prevent overwriting, erasing, or otherwise altering the records, during the applied retention period.

April 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 Pure Storage FlashBlade File Storage and the assessment scope.*

1.1 Overview of the Regulatory Requirements

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

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

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

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

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

1.1.2 FINRA Rule 4511(c) Requirements

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

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

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

---

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

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

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

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

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

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

1.2 Purpose and Approach

To obtain an independent and objective assessment of the compliance capabilities of FlashBlade File Storage for preserving required electronic records, Pure Storage 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.

Pure Storage engaged Cohasset to:

- Assess the functionality of FlashBlade File Storage, 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 FlashBlade File Storage; see Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d);* and
- Prepare this Compliance Assessment Report, enumerating the assessment results.

In addition to applying the information in this Compliance Assessment Report, regulated entities must ensure that the combination of its policies, procedures and regulatory submissions, in conjunction with the functionality of implemented electronic recordkeeping systems, meet all applicable requirements.

This assessment represents the professional opinion of Cohasset and should not be construed as either an endorsement or a rejection, by Cohasset, of FlashBlade File Storage and its functionality or other Pure Storage products or services. The information utilized by Cohasset to conduct this assessment consisted of: (a) oral discussions, (b) product demonstrations, including system setup and configuration, (c) system documentation, (d) user and system administrator guides, and (e) related materials provided by Pure Storage 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 FlashBlade File Storage Overview and Assessment Scope

1.3.1 FlashBlade File Storage Overview

Pure Storage FlashBlade is a highly-scalable, integrated solution designed for high-performance data storage on all-flash hardware. FlashBlade is a unified file and object storage platform, though this report assesses only FlashBlade File Storage.

The logical architecture of FlashBlade File Storage is depicted in Figure 1 and summarized as follows:

- **NFS and SMB Protocols:** FlashBlade File Storage supports NFSv3, NFSv4.1 and SMB file protocols.
- **Core Services:** The Core Services software layer is responsible for critical functions, such as the Purity//FB service, which manages, distributes and optimizes metadata and data for advanced file and object services.
- **Flash File System:** Files[4] are stored in file systems, using flash storage. For compliance with the SEC Rules, the WORM Status must be *enabled* on the file system (i.e., a *WORM-enabled* file system) and associated mandatory settings must be configured.
- **Files:** Files are stored in a file system. A *WORM-enabled* file system applies highly-restrictive retention controls when a Retain Until Date is applied and stored for the file. A *WORM-enabled* file system can also store files without retention controls.

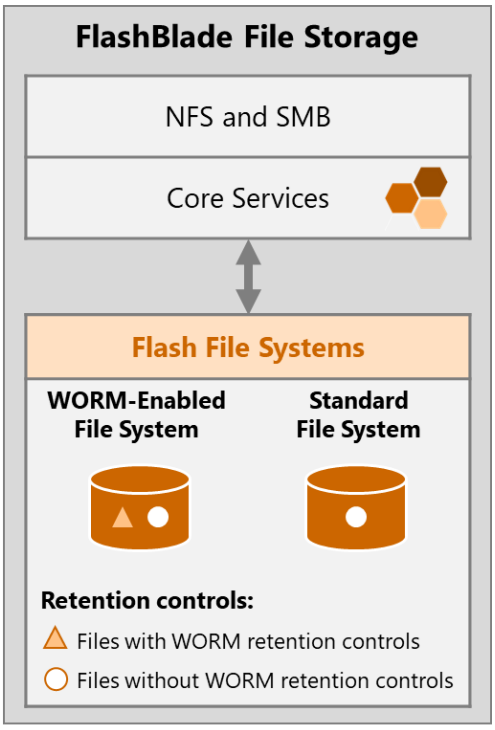

Figure 1: File Storage Architecture

1.3.2 Assessment Scope

This report assesses Pure Storage FlashBlade™ (including FlashBlade//S and FlashBlade//E) integrated hardware and software solutions deployed on-premises with Purity//FB release 4.5.5, when (a) the file system is *WORM-enabled* and (b) the associated compliance capabilities are properly configured and applied.

NOTES:

- As of the date of this report, a *WORM-enabled* file system can apply only highly-restrictive retention controls. Any future development of a less-restrictive mode has not been assessed for compliance with the SEC Rules.
- Software as a Service (SaaS) solutions using FlashBlade File Storage, when a third party manages or provides the solution to a regulated entity, are excluded from this report. Additionally, software-only FlashBlade products are not available.
- FlashBlade File Storage in a dedicated cloud not hosted by Pure Storage is excluded from this report.

[4] 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 or data, to recognize that the content may be required for regulatory compliance.

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

This section presents Cohasset's assessment of the functionality of Pure Storage FlashBlade File Storage, 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 FlashBlade File Storage
- ***FlashBlade File Storage 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 FlashBlade File Storage, as described in Section 1.3, *FlashBlade File Storage Overview and Assessment Scope*, relative to the enumerated requirements of SEC Rules 17a-4(f) and 18a-6(e).

2.1 Record and Audit-Trail

2.1.1 Compliance Requirement

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

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

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

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

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

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

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

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

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

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

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

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

2.1.2 Compliance Assessment

In this report, Cohasset has not assessed FlashBlade File Storage 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 FlashBlade File Storage, 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.

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

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

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

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

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

2.2.2 Compliance Assessment

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

Reminder: This 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 FlashBlade File Storage Capabilities

This section describes the functionality of FlashBlade File Storage 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

- To meet the non-rewriteable, non-erasable record format requirement of the SEC Rules, records requiring time-based retention must be stored in a *WORM-enabled* file system and retention controls must be applied to the required record (file).

---

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

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

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

- The following table summarizes the highly-restrictive retention controls applied to files in *WORM-enabled* file systems. See the subsections following this *Overview,* for information on configuring the retention features (Section 2.2.3.2, *FlashBlade File Storage Retention-related Configurations*) and the resulting integrated controls (Section 2.2.3.3, *Record Definitions and Controls*).

	***WORM-enabled* file systems**
Protecting record content and immutable metadata	● The file contents and immutable metadata cannot be modified or overwritten when the file (a) is stored in a *WORM-enabled* file system, (b) write permissions are removed, and (c) retention controls are applied. ● For a *WORM-enabled* file system ○ Renaming the file system, directories, folders and files is prohibited. ○ Restoring (i.e., promoting) a snapshot is prohibited. Therefore, a *WORM-enabled* file system cannot be overwritten by a snapshot.
Restricting changes to retention controls	● Retention controls cannot be circumvented by any user or process: ○ The WORM features cannot be removed from a *WORM-enabled* file system. ○ The Retain Until Date applied to a file can be extended at any time, though it cannot be reduced or removed. ● Additionally, the WORM Policy can be *Locked* to prohibit changes to the Default, Minimum and Maximum retention periods, as described in the row entitled "WORM Policy in Section 2.2.3.2, *FlashBlade File Storage Retention-related Configurations*. ● See Section 2.2.3.3, *Record Definition and Controls,* for descriptions of these controls.
Applying and removing legal holds	● Legals Holds can be applied to a root directory, specific directory or file, to prohibit modification and suspend deletion eligibility of the associated files until the Legal Hold attribute is cleared (removed). ● After all applied Legal Holds impacting a file are removed: ○ If a Retain Until Date has never been applied to the file, it can be modified, overwritten or deleted. ○ If a Retain Until Date has been applied to the file, the file cannot be modified or overwritten, and the file's Retain Until Date applies retention controls. ● See Section 2.2.3.4, *Legal Holds (Temporary Holds).*
Restricting deletion of file systems and records	● Deleting individual files and associated immutable file attributes are prohibited until both (a) the applied Retain Until Date is expired (i.e., the Retain Until Date is in the past) and (b) applicable Legal Holds are removed. ○ The applied Retain Until Date cannot be reduced, removed or circumvented by any user or administrator. ● Deleting a directory and subdirectory is prohibited, unless it is empty. ● Eradicating (permanently deleting) a *WORM-enabled* file system and associated files is prohibited. ● See Section 2.2.3.5, *Deletion Controls.*

2.2.3.2 FlashBlade File Storage Retention-related Configurations

- In FlashBlade File Storage, file systems store records, which can be logically organized into directories, subdirectories, and folders.
- The following table describes file system configurations required to apply highly-restrictive retention controls to files and associated immutable file attributes. See Section 2.2.3.3, *Record Definition and Controls,* for details on the integrated controls that these configurations apply to associated files.

	***WORM-enabled* file system configurations**
File system and path name	• Each file system must be assigned a unique path and file system name, which cannot be changed after the WORM Status is *enabled.* (See WORM Status row for details on this configuration.)
Protocols	• The file system protocol settings include NFS, SMB and Shared multi-protocol option (to permit both NFS and SMB).
WORM Status	• The WORM Status must be *enabled* (the WORM check-box must be selected) during file system creation, and once *enabled*, the setting cannot be changed or removed. Note: A file system with the WORM Status *enabled* are referred to as a *WORM-enabled* file system. • Enablement of the WORM Status on a file system requires a WORM Policy to be assigned. (See row labeled *WORM Policy,* below.) • Note: As of the date of this report, a WORM-enabled file system applies highly-restrictive retention controls (often referenced as *'Compliance'* mode). Any future development of a less-restrictive mode has not been assessed for compliance with the SEC Rules.
WORM Policy	During creation of a *WORM-enabled* file system, one WORM Policy must be assigned. A single WORM Policy can be assigned to multiple *WORM-enabled* file systems, which establishes consistency across multiple file systems. The mandatory configurations for a WORM Policy follow. 1. **Default Retention Period** is set in minutes, hours, days, months or years and must be configured within the guardrails of the Minimum and Maximum Retention Periods. The current Default Retention Period may be added to the current server timestamp to calculate a file's Retain Until Date, as described in Section 2.2.3.3, *Record Definition and Controls*. ○ Changes to the Default Retention Period apply to new files only and have no impact on the Retain Until Dates of previously stored files. See **Retention Lock** setting, below, for controls related to changing the Default Retention Period. 2. **Minimum** and **Maximum Retention Periods** is set in minutes, hours, days, months or years and must be configured to define the guardrails that validate both (a) the Default Retention Period and (b) the explicit Retain Until Dates transmitted using the Atime[10] file attribute. ○ Changes to the Minimum and Maximum Retention Periods apply going forward and have no impact on previously stored Retain Until Dates. See **Retention Lock** setting, below, for controls related to changing the Minimum and Maximum Retention Periods. 3. **Retention Lock** must be set to either *Locked* or *Unlocked*. ○ When *Locked*, the Default, Minimum and Maximum Retention Periods set in the WORM Policy cannot be changed (cannot be reduced and cannot be extended) by any user. ▪ Regulated entities can request Pure Storage support personnel to downgrade the *Locked* status to *Unlocked*. ○ When *Unlocked*, the Default, Minimum and Maximum Retention Periods set in the WORM Policy can be changed (reduced or extended) by an administrator. ▪ Administrators can change the *Unlocked* status to *Locked*. ○ Note: The current Default, Minimum and Maximum Retention Periods are used when setting Retain Until Dates. Changes to the Default, Minimum and Maximum Retention Periods do not affect previously stored files. Accordingly, either the *Locked* or *Unlocked* setting can be configured for compliance with the SEC Rules.

[10] Before WORM retention controls are applied to the file, the file's Atime attribute tracks the last time a file was accessed. For WORM-enabled file systems, when retention controls are applies to a file, the file's Atime attribute is repurposed to track the file's Retain Until Date.

2.2.3.3 Record Definition and Controls

- A record is an individual file with a unique file name within the directory where it is stored. It is comprised of:
  - The complete content of the file.
  - File attributes, which include:
    - Immutable (unchangeable) metadata: File system name, full directory path name, file name, extended attributes in NFS v4.1, creation (storage) timestamp, and last modified timestamp, which becomes immutable after a Retain Until Date is applied to the file.
    - Mutable (changeable) metadata: Retain Until Date (i.e., Atime), which can be extended but not reduced, and the Legal Hold attribute.
- To apply retention controls to a required record (a.k.a., file), the Retain Until Date is explicitly applied to the file and the file is stored in a *WORM-enabled* file system; thereafter, the file cannot be modified or overwritten for is lifespan.
- A single *WORM-enabled* file system can be configured to use NFS, SMB or both protocols and can store a combination of files with retention controls and other files without retention controls.
- The following table summarizes the combination of file attributes (columns with orange highlighted headings) and the impact on the file when committed for storage on a WORM-enabled file system (column with blue highlighted heading).

Write Permissions[11]	Atime[12]	Retention attributes stored for the file
Removed	Future	• The Atime value sets and stores the Retain Until Date for the file and the commitment process succeeds, *unless the guardrails set by the Minimum and Maximum Retention Periods are not met*. • Note: The commitment process fails, and the file is stored without retention controls (the write permissions are not removed and the Retain Until Date is not set in the Atime attribute), when the Minimum and Maximum Retention guardrails are not met because the transmitted Atime is either: ○ Greater than the current server timestamp plus the Maximum Retention Period, or ○ Less than the current server timestamp plus the Minimum Retention Period.
Removed	Past	• The *current server timestamp* + ***Default*** *Retention Period* sets the Retain Until Date for the file; the commitment process succeeds.
Permitted	Future	• The file is stored **without** retention controls (the write permissions are not removed and the Retain Until Date is not set in the Atime attribute).
Permitted	Past	

[11] When using the SMB protocol, setting the Boolean Read-Only attribute to Yes commits the file WORM-Protection. When using the NFS protocol, removing the chmod write permissions commits the file to WORM-Protection. Note: For NFS, changing the access control lists (ACLs) does not commit the file to WORM-Protection.

[12] Atime (a.k.a., last access time) is transmitted for the record (file) and is evaluated to determine if the Atime will set and store the file's Retain Until Date.

- The following table describes the integrated retention controls applied to files in a *WORM-enabled* file system, when the file is stored with retention attributes.

	Retention controls for files in a *WORM-enabled* file system
Uniquely identifying records	● The unique identifier for a record is immutable and is the combination of file system, full directory path, and file name. ● The file's creation (storage) timestamp is system generated and immutable. ● The file's last modified timestamp is system generated and immutable, after retention controls are applied.
Managing versions and protecting record content	● Versioning is not supported. ● After a Retain Until Date is applied to the file, (a) write capabilities are disabled and (b) the contents and immutable file attributes are immutably stored for the file's lifespan. If only a Legal Hold is applied to the file and it has never had a Retain Until Date applied, when the Legal Holds are removed, the file contents can be modified or overwritten. ● The file and its immutable file attributes can be deleted after the Retain Until Date is expired (i.e., the Retain Until Date is in the past) and all applicable Legal Holds have been removed.
Modifying or removing file retention attributes	● After the WORM features are enabled on a file system (a.k.a. WORM-enabled file system), the WORM features cannot be removed or disabled by any user or administrator. ● A *WORM-enabled* file system can store (a) files with highly-restrictive retention controls and (b) files without retention controls. ● Retention controls on a file are set by (1) removing the ability to write to the file by (i) setting the Boolean Read Only attribute (using SMB) or (ii) removing write permissions from the access control list (using NFS) and (2) applying a Retain Until Date, which is stored as the file's Atime value. ● Retention controls can be applied to (a) new files, (b) existing files without previously set retention controls, and (c) existing files with expired retention controls. ● When retention controls are applied to a file, the *WORM-enabled* file system applies highly-restrictive retention controls. Note: Any future development of a less-restrictive mode has not been assessed for compliance with the SEC Rules. ● After a Retain Until Date is applied to a file: ○ The file's write permissions cannot be reenabled. ○ The file's Retain Until Date can be extended, at any time, by setting a new Atime value that is further in the future. Extending a record's Retain Until Date does not affect the value of the record's last modified timestamp. ○ The file's Retain Until Date cannot be reduced.
Changing legal hold status	● One or more Legals Holds can be applied to a root directory, specific directory or file, which suspends deletion eligibility of the associated files until the Legal Hold attribute is cleared (removed). ● Applied Legal Holds can be removed. ● See Section 2.2.3.4, *Legal Holds (Temporary Holds)*.
Restricting deletion	● All attempts to **delete** a file, prior to the expiration of the Retain Until Date and removal of all Legal Holds, are rejected. ● No users are allowed to shorten or remove the Retain Until Date or delete an unexpired file. ● See Section 2.2.3.5, *Deletion Controls,* for additional information.
Copying records	● A file can be **copied** to a different file system. ○ The creation timestamp of the copy reflects the date and time that the copy is stored in the destination file system (not the date and time the file was originally stored in the source file system). ● Retention controls and Legal Holds must be separately applied to the new copy, in accordance with the configurations of the file system where the new copy is stored.

	Retention controls for files in a *WORM-enabled* file system
Moving records	● A record cannot be **moved** to a different file system. ● Note: If moves were allowed, retention controls would be jeopardized, when the new file system's retention features are different.
Handling symbolic links (symlinks)	● A symbolic link (symlink) directs the file system to the path of another file or directory. ○ Symlinks are not automatically updated when the associated file or directory is moved or deleted; therefore, links may point to a nonexistent files and directories. ● A Retain Until Date and Legal Hold can be applied to a symlink, which mandates retention of the symlink but does not mandate retention of the associated file or directory.
Handling hard links	● A hard link creates another name for (pointer to) an existing file on the same file system. ● The original file and the hard link share the same retention controls. ● Deleting the original file does not affect the hard link, and vice versa. The file is deleted after the original and all hard links to the file are deleted.
Changing permissions	● Read permissions can be changed (expanded or contracted) at any time. ● Write permissions cannot be reenabled after retention controls are applied to the file.
Restricting snapshot restores	● A snapshot is inextricably linked to its source directory. The snapshot establishes a virtual archive of files that existed at the snapshot's system-generated creation timestamp. ● Restoring (i.e., promoting) a snapshot in a *WORM-enabled* file system is prohibited. Therefore, a *WORM-enabled* file system cannot be overwritten by a snapshot. ● Note: If restoration were allowed, the file system contents would be overwritten by a previously created snapshot, potentially changing and deleting files.

2.2.3.4 Legal Holds (Temporary Holds)

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

	Legal Hold Features for *WORM-enabled* file systems
Creating a Legal Hold	● When creating a Legal Hold, the Legal Hold ID/Name and Description are entered. ○ The Legal Hold ID/Name is required and must be unique. ○ The Description parameter may track additional details useful for the administrator. Note: Cohasset recommends entering general (not private or confidential) information in these attributes, since administrators can view this content.
Applying Legal Holds	● One or more Legals Holds can be applied to: ○ A file, to prohibit modification and deletion of the explicit file. ○ A specific directory or to a root directory (i.e., file system) to: ▪ Prohibit modification and deletion of all files stored in the directory. ▪ Prohibit storage of new files in the directory.
Clearing Legal Holds	● When explicitly applied to files, the Legal Hold must be removed from each file. ● When explicitly applied to a root directory or a specific directory, removing the Legal Hold from the directory removes the Legal Hold controls for all subdirectories, folders and files in the directory.
Legal Hold protections	● A Legal Hold applied to a file prohibits modification and deletion of the explicit file. ● A Legal Hold applied to a specific directory or to a root directory (i.e., file system):

	Legal Hold Features for *WORM-enabled* file systems
	○ Prohibits modification and deletion of all files stored in the specific or root directory. ○ Prohibits storage of new files in the specific directory or root directory (i.e., file system). ● After all applied Legal Holds impacting a file are removed: ○ If a Retain Until Date has never been applied to the file, it can be modified, overwritten or deleted ○ If a Retain Until Date has been applied to the file, the file cannot be modified or overwritten, and the file's Retain Until Date controls retention and deletion eligibility.

2.2.3.5 Deletion Controls

- While deletion is not required by the SEC Rules, a file, together with its metadata, is eligible for deletion, when (a) its Retain Until Date is expired and (b) any Legal Holds applied to the file are removed.
- The following table summarizes actions taken to delete files.

	Deletion on *WORM-enabled* file systems
Deleting records	● For files stored in a *WORM-enabled* file system: ○ Authorized users and lifecycle actions can delete a specific file when both (a) the Retain Until Date is expired (i.e., the Retain Until Date is in the past) and (b) any appliable Legal Holds have been removed. Otherwise, the attempt to delete is rejected. ○ The Retain Until Date cannot be removed or circumvented by any user or administrator. ○ Deleting a directory and subdirectory is prohibited, unless it is empty. Note: Files without retention protection and without an applied Legal Hold are eligible for deletion at any time.
Deleting file systems	● A *WORM-enabled* file system cannot be eradicated (permanently deleted), even if it is empty. ● A *WORM-enabled* file system can be set to a destroyed status, which marks the file system, its contents (i.e., directories, subdirectories, folders and files) as deleted but does not eradicate (permanently delete) the file system and its contents.
Restricting snapshot restores	● Restoring (i.e., promoting) a snapshot of a *WORM-enabled* file system is prohibited. Therefore, a *WORM-enabled* file system cannot be overwritten by a snapshot. ● Note: If restoration were allowed, the file system contents would be overwritten by a previously created snapshot, potentially changing and deleting files.
Fast Remove	● The Fast Remove feature is disabled on a *WORM-enabled* file system, and therefore, its use is prohibited.
Secure erase	● If all retention protected files on the WORM-enabled file systems on a FlashBlade system/array are deleted, Pure Storage offers storage media sanitization services (crypto-erase), which is a verified secure erase process.
Factory reset	● Similar to decommissioning a storage solution, the Factory Reset process wipes the storage devices, after it has been confirmed that all the records have been deleted. ● An administrator cannot run the manual Factory Reset process, without active supervision of Pure Storage and only after multiple confirmations that the array is ready to be reset.

2.2.3.6 Security

In addition to the stringent retention and management controls described above, Pure Storage FlashBlade File Storage provides the following security capabilities, which support the authenticity and reliability of the records.

- FlashBlade File Storage employs a hardware implementation of the AES-256 algorithm to provide always-on, at-rest encryption of stored data and metadata. Encryption cannot be disabled. Each storage unit on a blade uses a unique device key to encrypt incoming data before storing it in flash, and to decrypt stored data for delivery to clients. Storage units hold their device keys in encrypted form in special-purpose flash, using a system-wide key encrypting key (KEK) to encrypt them. Device keys are never exposed outside storage units.
- When storage media is decommissioned, FlashBlade File Storage offers storage media sanitization services (crypto-erase), to ensure that data cannot be recovered.

2.2.3.7 Clock Management

- Regulated entities must request Pure Storage support personnel to enable a setting that blocks FlashBlade File Storage administrators from changing system time and from changing or adding network time protocol (NTP) time sources.
  - After configuration, the regulated entity does not have access to FlashBlade File Storage system clock. Any manual adjustment must be led by Pure Storage support personnel. Automatic adjustments to align with NTP time sources are described below.
- To protect against the possibility of premature deletion of records that could result from accelerating the system time clock, FlashBlade File Storage is configured to automatically check against the external NTP time source (approximately every one minute).
  - When the time difference between FlashBlade File Storage system clock and NTP is less than 128 milliseconds FlashBlade time skew is adjusted automatically at a rate of one-half millisecond per second to match with the NTP clock time.
  - When the time difference between FlashBlade File Storage system clock and NTP is greater than or equal to 128 milliseconds for more than 15 minutes, FlashBlade File Storage system clock will be set to NTP clock time.
  - FlashBlade alerts the administrator when a NTP clock drift of more than 2.5 minutes is detected.

2.2.4 Additional Considerations

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

- Enabling the WORM feature and properly configuring file systems and WORM Policies for file systems that will store required records.
- Applying a Retain Until Date, which meets regulators' retention requirements, to each record (i.e., each file) to assure highly-restrictive retention controls are applied to the file. Note: While a Default Retention Period is a mandatory setting for a WORM policy, it will not automatically apply to all files stored in a *WORM-enabled* file system. Accordingly, a *WORM-enabled* file system can retain a combination of records with and without retention controls.
- Ensuring all records required for compliance with the Rules are successfully stored with retention controls, preferably within 24 hours of creation.

- Storing records requiring event-based[13] retention periods in a separate compliant system, since FlashBlade File Storage does not currently support event-based retention periods.
- Applying Legal Holds or otherwise protecting files that require preservation for legal matters, government investigations, external audits and other similar circumstances and removing the Legal Holds when preservation is no longer required. Applying Legal Holds at the file-level is preferred, since applying to the root directory or to a specific directory halts the ability to store new files in the location.
- Ensuring that NTP clock servers are appropriately configured and monitored and that FlashBlade File Storage administrators are blocked from changing NTP clock settings.

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.

2.3.2 Compliance Assessment

Cohasset affirms that the functionality of FlashBlade File Storage meets this SEC requirement for complete and accurate recording of records and post-recording verification processes, when properly configured as described in Section 2.3.3 and the considerations identified in Section 2.3.4 are satisfied.

2.3.3 FlashBlade File Storage Capabilities

The recording and post-recording verification processes of FlashBlade File Storage are described below.

2.3.3.1 Recording Process

- FlashBlade File Storage employs erasure coding to tolerate failures without data loss.
  - Erasure coding can be configured in N+2, N+3 or N+4 schemes, with higher numerical values resulting in increased redundancy and enhanced data protection.
- FlashBlade File Storage calculates and stores a checksum for each data segment, which is used for post-recoding verification.

[13] 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.

2.3.3.2 Post-Recording Verification Process

- Multiple background processes run automatically to identify errors and correct detected corruption.

2.3.4 Additional Considerations

- The source system is responsible for transmitting the complete contents of the required records and FlashBlade File Storage validates the accuracy of the recording process.

2.4 Capacity to Download and Transfer Records and Location Information

2.4.1 Compliance Requirement

SEC 17a-4(f)(2)(iv) and 18a-6(e)(2)(iv):
Have the capacity to readily download and transfer copies of a record and its audit-trail (if applicable) in both a human readable format and in a reasonably usable electronic format and to readily download and transfer the information needed to locate the electronic record, as required by the staffs of the Commission, [and other pertinent regulators] having jurisdiction over the [regulated entity]

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

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

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

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

2.4.2 Compliance Assessment

Cohasset asserts that the functionality of FlashBlade File Storage 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 FlashBlade File Storage Capabilities

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

- Each record's unique identifier is immutable and facilitates findability. Specifically, when using the NFS or SMB protocols, the immutable unique identifier is the combination of (a) File system name, (b) Full path, including directories, subdirectories and folders, and (c) File name.
- In addition, after retention controls are applied to a file, its last modified and creation (storage) timestamps are immutable for the lifespan of the file.
- The file's Atime attribute applies, stores and displays the file's current Retain Until Date, which can be extended, but cannot be reduced or removed.

- Files stored in a *WORM-enabled* file system can be located as follows:
  - Authorized users can navigate the directory and file structure.
  - Protocol-specific lookup operations can be used to access stored files and associated attributes.
- FlashBlade File Storage assures that hardware and software capacity allow for ready access to the records and associated file attributes.

2.4.4 Additional Considerations

Additionally, the regulated entity is responsible for: (a) authorizing user permissions, (b) maintaining appropriate technology and resource capacity, encryption keys, and other information and services needed to use FlashBlade File Storage 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.[14] [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.[15] [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.

[14] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66421.

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

2.5.2 Compliance Assessment

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

2.5.3 FlashBlade File Storage Capabilities

- For compliance with paragraph (B), FlashBlade File Storage uses erasure coding to store data segments that are distributed across the available blades for redundancy. The erasure coded data is retained for the full retention period of the record and any applied Legal Holds.
- Erasure coding is configured automatically, by the Purity//FB software. Based on the system configuration, erasure coding is configured as N+2, N+3 or N+4 redundancy schemes, with higher numerical values resulting in increased resiliency and enhanced data protection.
- A replica of the files can be accurately regenerated from the erasure coded data segments in the event of a blade failure.

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 FlashBlade File Storage 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 FlashBlade File Storage, in conjunction with Pure Storage management logs supports the regulated entity's efforts to meet this SEC requirement for an audit system.

2.6.3 FlashBlade File Storage Capabilities

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

- For each file stored in a WORM-enabled file system, when retention controls are applied to the file, FlashBlade File Storage retains the following immutable audit attributes for the lifespan of the file.
  - Unique identifier for each file, which is comprised of (a) File system name, (b) Full path, including directories, subdirectories and folders, and (c) File name.
  - The file's creation (storage) timestamp, which chronologically accounts for each file.
  - The file's last modified timestamp, which becomes immutable after retention controls are applied to the file.

  These immutable attributes can be viewed for the file and may be produced together with the file.
- Additionally, the file's Atime attribute applies, stores and displays the file's current Retain Until Date, which can be extended, but cannot be reduced or removed.
- When retention controls are applied to the file, the associated record content is immutably stored over its lifespan; changes to the file's content are not allowed.
  - Accordingly, tracking of the inputting of changes made to the record content is not relevant to records stored in a *WORM-enabled* file system, when retention controls applied to the file.
- In addition, management logs track each management activity performed on a file system, including, but not limited to file system creation, configuration and deletion.
  - Management log events are immutable once created.
  - Administrators access the management logs using the REST APIs or command line interface.
- The management logs can be exported for (a) ingestion by a centralized logging server or (b) storage in a specified destination. These separate storage locations can be leveraged to retain the management log events for the same time period as the associated record.

2.6.4 Additional Considerations

The regulated entity is responsible for maintaining an audit system for inputting records and changes made to the records. In addition to relying on the immutable file attributes, the regulated entity may utilize the management logs. When relying on the management logs, Cohasset recommends copying the management logs to a security information event management tool.

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

This section contains a summary assessment of the functionality of FlashBlade File Storage, as described in Section 1.3, *FlashBlade File Storage 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.*[16] [emphasis added]

In Section 2 of this report, Cohasset assesses FlashBlade File Storage, when the *WORM-enabled* file system is properly configured, and retention controls are applied to the file. The retention controls for a *WORM-enabled* file systems apply highly restrictive integrated controls to (a) prevent modifications to the record content and certain immutable file attributes and (b) prevent deletion over the applied retention period.

In the following table, Cohasset correlates specific *principles-based* CFTC requirements for electronic records with the functionality of FlashBlade File Storage, when the *WORM-enabled* file system is properly configured, and retention controls are applied to the file. The first column enumerates the CFTC regulation. The second column provides Cohasset's analysis and opinion regarding the ability of FlashBlade File Storage, relative to these requirements.

[16] 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[17] with time-based retention periods, are met by the functionality of FlashBlade File Storage, when the *WORM-enabled* file system is properly configured and retention controls are applied to the file. 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] FlashBlade File Storage retains immutable attributes as an integral component of the files, and, therefore, these attributes are subject to the same retention controls as the associated record. These immutable attributes support both (a) records access, search and display and (b) audit system and accountability for inputting the records. The immutable metadata include the following: ● Unique identifier for each file, which is comprised of: ○ File system name, ○ Full path, including directories, subdirectories and folders, and ○ File name. ● The file's creation (storage) timestamp, which chronologically accounts for each file. ● The file's last modified timestamps, which becomes immutable after retention controls are applied to the file. Additionally, when retention controls are applied to the file the Retain Until Date can be extended, though not reduced. Separately, Legal Holds can be applied to (and subsequently removed from) directories, subdirectories, folders or files stored in *WORM-enabled* file systems. The most recent values of these mutable attributes are retained for the same time period as the associated records.

[17] 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)**
(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 FlashBlade File Storage capabilities described in Section 2.5, *Record Redundancy*, which describe methods for an alternate source to reestablish the files and associated file attributes, meet the CFTC requirements (c)(2)(ii) to *ensure the availability of such regulatory records in the event of an emergency or other disruption of the records entity's electronic record retention systems*.
(iii) The creation and maintenance of an up-to-date inventory that identifies and describes each system that maintains information necessary for accessing or producing electronic regulatory records.	The regulated entity is required to create and retain an *up-to-date inventory,* as required for compliance with 17 CFR § 1.31(c)(iii).
(d) Inspection and production of regulatory records. Unless specified elsewhere in the Act or Commission regulations in this chapter, a records entity, at its own expense, must produce or make accessible for inspection all regulatory records in accordance with the following requirements: *(1) Inspection. All regulatory records shall be open to inspection by any representative of the Commission or the United States Department of Justice.* *(2) Production of **paper** regulatory records. **** *(3) Production of **electronic** regulatory records.* *(i) A request from a Commission representative for electronic regulatory records will specify a reasonable form and medium in which a records entity must produce such regulatory records.* *(ii) A records entity must produce such regulatory records in the form and medium requested promptly, upon request, unless otherwise directed by the Commission representative.* *(4) Production of **original** regulatory records. ****	It is Cohasset's opinion that FlashBlade File Storage has features that support the regulated entity's efforts to comply with requests for inspection and production of records, as described in. ● Section 2.2, *Non-Rewriteable, Non-Erasable Record Format* ● Section 2.4, *Capacity to Download and Transfer Records and Location Information* ● Section 2.6, *Audit System*

4 • Conclusions

Cohasset assessed the functionality of *WORM-enabled* file systems for FlashBlade File Storage[18] 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 FlashBlade File Storage, when properly configured, has the following functionality, which meets the regulatory requirements:

- Retains the records and immutable file attributes in non-rewriteable, non-erasable format for time-based retention periods when the files are stored in a *WORM-enabled* file system and a Retain Until Date is applied to the file.
- Permits Legal Holds to be applied to directories, subdirectories, folders or individual files stored in a *WORM-enabled* file system. The Legal Hold preserves the associated records for a subpoena, legal matters or similar circumstances, and permits removing the hold when the matter is released.
- Prohibits deletion of records until the Retain Until Date is expired and any applied Legal Holds are removed.
- Verifies the accuracy of the recording processes, calculates and stores a checksum for each data segment, and uses the checksums for post-recoding validation processes to identify errors and correct detected corruption.
- Provides authorized users with the capacity and tools to readily (a) navigate the directory and file structure, (b) use protocol-specific lookup operations to access stored files and associated attributes, and (c) download selected records and associated file attributes for a local tool to produce a human readable image and a reasonably usable electronic format.
- Maintains records redundancy to regenerate an accurate replica of the record from the erasure coded data should an error occur, or an availability problem be encountered.
- Supports the regulated entity's obligation to retain an audit system for non-rewriteable, non-erasable records.

Accordingly, Cohasset concludes that *WORM-enabled* file systems, using FlashBlade File Storage, 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).

[18] See Section 1.3, *FlashBlade File Storage 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[19] 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.*[20] [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.*[21] [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.

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

[20] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66428.

[21] 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.*[22] [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.*[23] [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."*[24] [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****[25] [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).

---

22 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.
23 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.
24 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66418.
25 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.*[26] [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.*[27] [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.*[28] [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 FlashBlade File Storage 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).[29]

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.*

---

26 2003 Interpretative Release, 68 FR 25282.

27 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).

28 2003 Interpretative Release, 68 FR 25283.

29 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.*[30] [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 FlashBlade File Storage in relation to each requirement, see Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*.

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

About Cohasset Associates, Inc.

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

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

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

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

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

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

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.