Cohasset Associates

Pure Storage® FlashBlade® Object 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 Object Storage. The Object Lock retention features, together with other compliance capabilities, are designed to meet securities industry requirements for preserving records in non-rewriteable, non-erasable format for the applied retention period and legal holds.

In this report, Cohasset Associates, Inc. (Cohasset) assesses the functionality of FlashBlade Object Storage (see Section 1.3, *FlashBlade Object 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 Object Storage, when properly configured and used with Object Lock retention features and other compliance capabilities, 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 Object 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.

May 2024

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 Object 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 Object 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 Object 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 Object 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 Object 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 Object Storage Overview and Assessment Scope

1.3.1 FlashBlade Object 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 Object Storage.

FlashBlade Object Storage is designed for S3-compatibility. The logical architecture is depicted in Figure 1 and summarized as follows:

- **S3-Compatible API:** FlashBlade Object Storage adheres to the S3 API (application programming interface) standards.
- **HTTP Server:** HTTP (Hypertext Transfer Protocol) is the underlying stateless protocol used for communication and data transfer, including use by the S3-Compatible APIs.
- **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 Object Storage:** Objects[4] and object versions are stored in Buckets.

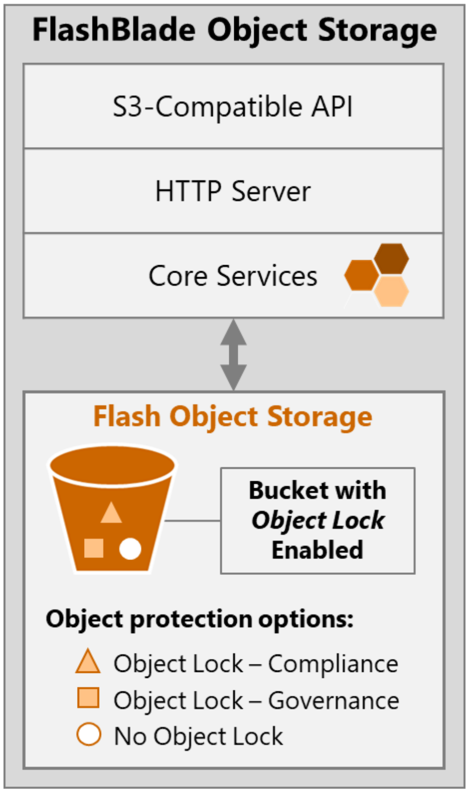
FlashBlade Object Storage
S3-Compatible API
HTTP Server
Core Services
Flash Object Storage
Bucket with *Object Lock* Enabled
Object protection options:
△ Object Lock – Compliance
□ Object Lock – Governance
○ No Object Lock

Figure 1: Object Storage Architecture

For compliance with the non-rewriteable, non-erasable requirement of SEC Rules 17a-4(f) and 18a-6(e), (a) the Object Lock feature must be enabled on the Bucket and (b) Object Lock retention controls must be applied to each required record. While FlashBlade Object Storage supports both highly-restrictive *Compliance* mode and less-restrictive *Governance* mode, this report assesses only records set to *Compliance* mode, which systemically disallows reducing or removing retention controls by any user.

[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 or record version*, in addition to specific terms, e.g., file, object, or object version, to recognize that the content may be required for regulatory compliance.

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 4.4.0, when (a) properly configured with the Object Lock feature and (b) highly-restrictive *Compliance* mode retention controls are applied to required records.

Notes:

- Software as a Service (SaaS) solutions using FlashBlade Object 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.
- Amazon S3 as a target location for asynchronous replication is also excluded from the scope of this assessment.
- Further, FlashBlade Object Storage supports the Object Lock feature applied in less-restrictive *Governance* mode. However, in this report, Cohasset assesses the more stringent retention controls provided in *Compliance* mode.

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 Object 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 Object Storage
- ***FlashBlade Object 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 Object Storage, as described in Section 1.3, *FlashBlade Object 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 Object 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 Object Storage, with the features and controls described in Sections 2.2 through 2.6 of this report.

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

2.2 Non-Rewriteable, Non-Erasable Record Format

2.2.1 Compliance Requirement

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

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

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

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

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

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

> *2019 interpretation further refined the 2003 interpretation. In particular, it noted that the 2003 interpretation described a process of integrated software and hardware codes and clarified that "<u>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</u>."*
>
> *****
>
> *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 <u>the broker-dealer's storage system must allow records to be retained beyond the retentions periods specified in Commission rules.</u>*[8] [emphasis added]

2.2.2 Compliance Assessment

It is Cohasset's opinion that the functionality of FlashBlade Object Storage, with Object Lock retention controls applied in *Compliance* mode, 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.

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

2.2.3 FlashBlade Object Storage Capabilities

This section describes the functionality of FlashBlade Object 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. <u>Note</u>: Throughout this report, the terms record (or object) refers to each record version (or object version), when Versioning is enabled.

2.2.3.1 Overview

- To meet the non-rewriteable, non-erasable record format requirement of the Rules, records requiring time-based retention must:
  - be stored in a Bucket with the Object Lock feature enabled, and <u>either</u>:
    - have Versioning <u>enabled</u>, which stores new versions when the record or its immutable metadata is modified, **<u>or</u>**

[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 requires records to be retained for a fixed contiguous period of time from the last modified (storage) timestamp.

    - have Freeze Locked Objects selected, which disallows versions and disallows modifications to the content of stored records and associated immutable metadata,
  - have a Retention Mode of highly-restrictive *Compliance* applied to each record or record version, if Versioning is enabled; and
  - have an appropriate Retain Until Date applied to each record or record version.
- Optionally, a Legal Hold attribute may be set (On) which suspends deletion eligibility until the Legal Hold attribute is cleared (No).
- The following table summarizes the retention controls resulting from applying Object Lock retention controls in highly-restrictive *Compliance* mode. See the subsections following this *Overview*, for information on configuring the retention features and the resulting integrated controls.

	Object Lock retention controls applied, in highly-restrictive *Compliance* mode
Protecting record content and immutable metadata	● By design, each record and its immutable attributes cannot be modified for its lifespan. ○ When Versioning is enabled, modifications result in storing a new record version. ○ When Freeze Locked Objects is selected (i.e., Versioning not allowed), any attempt to modify or overwrite an object fails. ● Renaming an object or version ID is prohibited. ● Manually setting or changing the last modified (storage) timestamp is prohibited. ● Renaming a Bucket with Object Lock enabled is prohibited.
Restricting changes to retention controls	● *Compliance* mode, when applied to a record (i.e., an object or object version), cannot be removed and cannot be downgraded to *Governance* mode. ● The Retain Until Date applied to a record may be extended at any time, though it cannot be reduced or removed. ● Accordingly, *Compliance* mode assures retention controls are not circumvented by any user or process. ● Additionally, default values for a Bucket with Object Lock enabled (e.g., Default Retention Mode, Default Retention Period) can be locked via the Retention Lock feature in *Ratcheted/Locked* (i.e., *SafeMode*) status. When Safe Mode is configured for a Bucket, any changes to applied default values require multi-party authorization. ● See Section 2.2.3.3, *Record Definition and Controls.*
Applying and removing Legal Holds	● To preserve records for a hold, the Legal Hold attribute is set (Yes) and may be set whether or not retention attributes are applied to the record. ● See Section 2.2.3.4, *Legal Holds (Temporary Holds).*
Restricting deletion	● Deleting individual record versions and associated metadata is prohibited until the applied Retain Until Date expires and the Legal Hold attribute is clear (No). ○ *Compliance* mode retention controls cannot be removed or circumvented by any user or administrator. ● To prohibit eradication (permanent deletion) of the Bucket and deletion of the Bucket's objects, the Bucket's Eradication Mode must be set to *Retention-based.* ● See Section 2.2.3.5, *Deletion Controls.*

2.2.3.2 FlashBlade Object Storage Retention-Related Configurations

- In FlashBlade Object Storage, Buckets are logical containers that store records.
  - Within each Bucket, records are stored in a flat storage hierarchy. To help organize records, a folder structure can be simulated using a prefix string for object names (usually a slash "/").
- The following table describes Bucket configurations related to Object Lock and other features that allow a Bucket to retain records in highly-restrictive *Compliance* mode to meet the requirements of the Rules.

	Bucket configurations for *Object Lock* and related features
Bucket name	● Each Bucket with Object Lock enabled must be assigned a unique name, which cannot be changed.
Object Lock feature	● Enabling the Object Lock feature on a Bucket allows retention and Legal Hold controls to be applied to records or record versions stored in the Bucket. ● The Object Lock feature must be enabled on the Bucket when it is empty. ● Once enabled, Object Lock cannot be disabled for the Bucket.
Versioning and Freeze Locked Objects	● Two mutually exclusive features define version management. To safeguard the object either: ○ Enable Versioning. (This prohibits selection of Freeze Locked Objects.) ▪ When Versioning is enabled, modifications to records or immutable metadata result in storing a new version, with separate retention and Legal Hold attributes. ▪ A version ID is automatically stored as immutable metadata. ○ Select Freeze Locked Objects. (This prohibits enablement of Versioning.) ▪ When Freeze Locked Objects is selected, stored records and immutable metadata cannot be modified; modification attempts fail. ▪ A version ID is stored as immutable metadata for the initial (and only) version, and no additional versions are allowed. Actions are automatically taken on the current (and only) version; therefore, the version ID does not need to be stipulated. ● Pure Storage support personnel may simultaneously change (a) Versioning from not set to enabled and (b) Freeze Locked Objects from selected to unselected. These changes essentially enable new versions to be stored. No other changes to these configurations are allowed by Pure Storage support personnel or by administrators. ○ As explained for Freeze Locked Objects, above, a version ID is assigned to the initial version. Therefore, objects stored before and after the configuration change will have version IDs assigned. ○ After the change is made, behaviors are consistent with Versioning having been enabled before records are stored in the Bucket.
Default retention values	● Default retention values are optional and, if configured, must be set as a pair, requiring both or neither to be set. ○ The Default Retention Mode may be set to *Compliance* or *Governance*. Reminder: *Compliance* mode is the subject of this report. ○ The Default Retention Period may be set in terms of days, between 1 and 36,500 days (100 years). ▪ When these defaults apply, the Default Retention Period is added to the record's last modified (storage) timestamp to calculate a Retain Until Date which is stored as an attribute for the record. ● When configured, these defaults apply during storage/write operations to new record versions when an explicit Retention Mode and Retain Until Date are not transmitted with the record version. ● Notes: ○ Setting these Bucket defaults assures retention controls are applied when storing a record version. ○ See the row entitled *Retention Lock*, below, for an explanation of controls related to changing these default retention values. ○ This report assesses record versions set to *Compliance* mode; see Section 2.2.3.3 *Record Definition and Controls*, for additional information.

	Bucket configurations for *Object Lock* and related features
Retention Lock	● Retention Lock is a mandatory configuration and must be set to *Unlocked* or *Ratcheted/Locked* (i.e., *SafeMode*) status when the Bucket is empty. ● Retention Lock controls the process to change the Default Retention Mode and Default Retention Period on the Bucket. ○ When Retention Lock is set to *Unlocked*, any authorized administrator may change the Default Retention Mode and may reduce or extend the Default Retention Period. ○ When Retention Lock is set to *Ratcheted/Locked* (i.e., *SafeMode*) status: ▪ If the Default Retention Mode is currently set to *Compliance,* Pure Storage support personnel lead the operation to change the setting, after receiving multi-party authorization from the regulated entity: ▪ If the Default Retention Mode is currently set to *Governance* or *None*: • Any authorized administrator may change the Default Retention Mode and may reduce or extend the Default Retention Period. ● Notes: ○ Since these defaults only apply to records stored in the future and do not affect previously stored records, authorized users may change or remove these default configurations at any time, as described in the row above. ○ The *Ratcheted/Locked* (i.e., *SafeMode*) status limits who can change these default settings, offering enhanced control.
Eradication Mode	● For compliance with the Rules, Bucket Eradication Mode must be set to *Retention-based* to disallow eradication (permanent deletion) of the Bucket and deletion of all its records, whether the record's Retain Until Date is in the past or not. ● This configuration must be set when the Bucket is empty and the setting cannot be changed after objects are stored in the Bucket.

2.2.3.3 Record Definition and Controls

- When Versioning is enabled, each record version (i.e., object version) is managed as a separate record (i.e., object), with separate metadata, retention controls and legal holds. Each record is comprised of:
  - The complete content of the record, which is unmodifiable.
    - Immutable (unchangeable) metadata: Bucket name, object name and version ID, custom metadata, and last modified (storage) timestamp, as well as *Compliance* mode after it is applied.
    - Mutable (changeable) metadata: Retain Until Date (which can be extended, but not reduced, when the record is set to *Compliance* mode) and the Legal Hold attribute.
- For Buckets with Object Lock enabled, retention attributes (Retention Mode and Retain Until Date) and optional Legal Hold attributes are explicitly applied to each record version. A single Bucket may store records with a mix of *Compliance*, *Governance,* or no retention controls. Additionally, the Legal Hold attribute may be applied to records, independent of retention controls.
- The following table summarizes the retention attributes (Retention Mode and the Retain Until Date) applied during the initial storage process, based on (a) the retention attributes transmitted as a pair with the record version (columns with orange highlighted headings), (b) the Bucket's default retention settings (columns with blue highlighted headings). Reminder: For this assessment, the record's Retention Mode must be set to *Compliance*.

Transmitted Retention Mode	Transmitted Retain Until Date	Record version's retention attributes, when the Bucket has no default retention settings	Record version's retention attributes, when the Bucket has default retention settings
Null	MM/DD/YYYY	● Rejected; record creation fails because both retention attributes were not transmitted	
Null	Null	● Record version is stored **without** retention controls	● Record version is set to the Default Retention Mode (e.g., *Compliance*) and Retain Until Date is record version's last modified (storage) timestamp + Default Retention Period
Governance	MM/DD/YYYY	● Record version is set to *Governance* mode and Retain Until Date is MM/DD/YYYY	
Governance	Null	● Rejected; record creation fails because both retention attributes were not transmitted	
Compliance	MM/DD/YYYY	● Record version is set to *Compliance* mode and Retain Until Date is MM/DD/YYYY	
Compliance	Null	● Rejected; record creation fails because both retention attributes were not transmitted	

- For previously stored records without retention controls Retention Mode and Retain Until Date may be set, as a pair. If only one attribute is transmitted, the operation fails. As a reminder, only highly-restrictive *Compliance* mode is assessed in this report.
- In addition, the Retention Mode and Retain Until Date applied to a record may be modified, with certain limitations, as described in the following table, in the row labeled *Modifying or removing retention controls*.
- The following table describes the integrated retention controls applied to a record, when Object Lock features are applied to the record in highly-restrictive *Compliance* mode.

	Object Lock, in highly-restrictive *Compliance* mode
Protecting record content and immutable metadata	● The mutually exclusive features of Versioning and Freeze Locked Objects define version management and protect record content. ○ When Versioning is enabled, any attempt to modify or overwrite an object results in storing a new version, with separate retention controls. Each record version, together with its immutable metadata, is unmodifiable for its lifespan. ○ When Freeze Locked Objects is selected, any attempt to modify or overwrite an object fails, and the record together with its immutable metadata is unmodifiable for its lifespan.
Modifying or removing retention controls	● For record versions set to *Compliance* mode: ○ *Compliance* mode cannot be changed to *Governance* mode. ○ The Retain Until Date, can be extended at any time, but cannot reduced. ▪ If the version ID is explicitly identified, the updated retention attributes are applied to the explicit version. ▪ If the version ID is not explicitly identified, the updated retention attributes are applied to the current (top) record version. ○ The retention controls cannot be removed. ● Additionally, a record versions set to *Governance* mode can be changed to *Compliance* mode. ● Changes to the retention attributes do not generate a new version and do not affect the record version's last modified (storage) timestamp.
Changing Legal Hold attribute	● A record version's Legal Hold attribute can be set (Yes) or cleared (No), whether or not it has retention controls applied. See Section 2.2.3.4, *Legal Holds (Temporary Holds)*, for additional information.

	Object Lock, in highly-restrictive *Compliance* mode
Restricting deletion	● When Versioning is enabled: ○ All attempts to **delete** a record version (specifying a version ID), prior to the expiration of the Retain Until Date and clearing of any Legal Hold, are rejected. ○ All attempts to **delete** a record without specifying the version ID results in appending a Delete Marker as the current (top) version. The Delete Marker can be removed to reinstate the record. ● When Freeze Locked Objects is selected, attempts to **delete** a record or record version prior to the expiration of the Retain Until Date and clearing of any Legal Hold, are rejected. ● No users are allowed to shorten or remove the Retain Until Date or delete an unexpired record or record version. ● See Section 2.2.3.5, *Deletion Controls,* for additional information.
Copying records	● A record may be **copied** to a different Bucket. ○ The last modified (storage) timestamp of the copy reflects the timestamp when the copy is stored in the destination Bucket (not the timestamp when the object was originally stored in the source Bucket). ● Retention controls and Legal Hold attribute must be separately applied to the new copy, in accordance with the configurations of the Bucket where the new copy is stored.
Moving records	● A record cannot be **moved** to a different Bucket. ● Note: If moves were allowed, retention controls would be jeopardized if the new Bucket's retention features were different.

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 no longer applies.

► The following table describes the Legal Hold features for Buckets with Object Lock enabled.

	Object Lock features for Legal Holds
Applying and clearing Legal Holds	● The Legal Hold attribute may be applied (Yes) or cleared (No) for any record version stored in a Bucket with Object Lock enabled. ○ If no version is specified, the Legal Hold attribute update is applied to the current (top) version and if the current (top) version is a Delete Marker, the Legal Hold attribute is not updated. ● The Legal Hold attribute is independent of the record version's Retention Mode and Retain Until Date; therefore, a Legal Hold attribute may be applied to any record version in a Bucket with Object Lock enabled whether or not the record version has retention controls.
Legal Hold protections	● When the Legal Hold attribute is set (Yes) for a specific record version, deletion of the record version is prohibited until the Legal Hold attribute is clear (No). ● When the Legal Hold attribute is clear (No), this attribute no longer mandates preservation of the record version; however other retention controls continue to be enforced for the record version.

2.2.3.5 Deletion Controls

- While deletion is not required by the SEC Rule, a record version, together with its metadata, is eligible for deletion, when (a) its Retain Until Date has expired (is in the past) and (b) its Legal Hold attribute is clear (No).
- The following table summarizes actions taken to delete records and record versions.

	Record Deletion when Object Lock retention controls are applied, in highly-restrictive *Compliance* mode
Deleting records	● Authorized users may delete a specific record version and its associated immutable metadata only when both the Retain Until Date is expired (is in the past) and Legal Hold attribute is clear (No). Otherwise, deletion is rejected. ○ When set to *Compliance* mode, the retention controls cannot be removed or circumvented by any user or administrator. ● When an authorized user deletes a record, without identifying the version ID: ○ When Versioning is enabled, a Delete Marker is appended as the current (top) version (regardless of the record's deletion eligibility). This Delete Marker may be removed, at any time, to reinstate the original record and its versions. ○ When Freeze Locked Objects is selected, the deletion attempt succeeds only if both the Retain Until Date is expired (is in the past) and Legal Hold attribute is clear (No); otherwise, the deletion attempt fails.
Soft-deleting (Destroying) Buckets	● A Bucket may be soft-deleted (destroyed), which marks the Bucket as deleted but does not eradicate (permanently delete) the Bucket. ○ A soft-deleted Bucket may be reinstated at any time.
Eradicating Buckets	● For compliance with the Rules, Bucket Eradication Mode must be set to *Retention-based,* which prohibits automated and manual processes that eradicate (permanently delete) the entire Bucket and delete the Bucket's records. ● This configuration must be set when the Bucket is empty and the setting cannot be changed after objects are stored in the Bucket.
Secure erase	● 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 Object Storage provides the following security capabilities, which support the authenticity and reliability of the records.

- Role-Based Access Control (RBAC) is employed to allow administrators to restrict administrative access to credentialed individuals, each with a defined role that permits specific action, based on the principle of least privilege.
- Multi-party authorization is required, with certain configurations, to change default retention controls.
- FlashBlade Object 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.

- The Hypertext transport-layer encryption (HTTPS) protocol is used to protect data in transit.
- When storage media is decommissioned, FlashBlade Object 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 Object Storage administrators from changing system time and from changing or adding network time protocol (NTP) time sources.
  - After configuration, the regulated entity does <u>not</u> have access to FlashBlade Object 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 Object Storage is configured to automatically check against the external NTP time source (approximately every one minute).
  - When the time difference between FlashBlade Object 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 Object Storage system clock and NTP is greater than or equal to 128 milliseconds for more than 15 minutes, FlashBlade Object Storage system clock will be set to NTP clock time.
- FlashBlade also compares the system times of FlashBlade Object Storage to the source system (i.e., originating S3 application request). If the difference is 15 minutes or more, FlashBlade Object Storage (a) issues an alert and (b) blocks all S3 requests, including, but not limited, to writing new records and deleting records until the issue is corrected.

2.2.4 Additional Considerations

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

- Enabling the Object Lock feature and properly configuring Buckets that will store required records.
- Applying Retention Mode of *Compliance* and a Retain Until Date that meets regulators' retention requirements to each record (i.e., each record <u>version</u>). For Buckets that store records required for compliance with the Rules, Cohasset recommends configuring (a) an appropriate Default Retention Period and (b) Default Retention Mode of *Compliance,* to assure highly-restrictive retention controls are applied to all records stored in the Bucket.
- 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[10] retention periods in a separate compliant system, since FlashBlade Object Storage does not currently support event-based retention periods.
- Setting the Legal Hold attribute (Yes) or otherwise protecting records that require preservation for legal matters, government investigations, external audits and other similar circumstances and clearing Legal Hold attribute (No) when preservation is no longer required.
- Limiting the creation and management of Delete Markers. Specifically, Cohasset recommends always specifying the version ID with delete actions.
- Setting the Bucket's Eradication Mode to *Retention-based* to prohibit eradication (permanent deletion) of the Bucket and associated records.
- Setting appropriate security controls to (a) restrict network ports and protocol access, (b) establish roles-based access, and (c) encrypt data in transit.
- Ensuring that NTP clock servers are appropriately configured and monitored and that FlashBlade Object Storage administrators are blocked from changing NTP clock settings.

Additionally, the regulated entity is responsible for: (a) authorizing user permissions 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 Object 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 Object Storage Capabilities

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

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

2.3.3.1 Recording Process

- FlashBlade Object Storage employ error correction codes to detect and correct bit level data errors that occur during data transmission. Parity data is added to the original data, creating a code that is used to check for errors and make corrections, often without requiring data to be retransmitted.
- FlashBlade Object Storage calculates and stores a checksum for each data segment, which is used for post-recoding verification.
- FlashBlade Object 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.

2.3.3.2 Post-Recording Verification Process

- Multiple background processes run automatically to identify errors and correct detected corruption.
  - Background healing processes include recalculation of data segment checksums and comparison to the stored values.

2.3.4 Additional Considerations

The source system is responsible for transmitting the complete contents of the required records and FlashBlade Object 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 Object 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 Object Storage Capabilities

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

	Capabilities for the capacity to readily search, access, download, and transfer records
Uniquely Identifying Records	● Each record version's unique identifier is immutable for the lifespan of the record and facilitates findability: ○ The immutable unique identifier is the combination of Bucket name, object name and version ID. ○ The last modified (storage) timestamp is immutable when retention controls are applied. ● Each record version can be accessed separately.
Hardware and Software Capacity	● FlashBlade Object Storage assures that hardware and software capacity allows for ready access to the record versions and metadata attributes.
Locating records	● ListObject returns a list of the records, by Bucket name, object name and version ID. ○ If the most recent version is a Delete Marker the record is not returned in the list. ● ListObjectVersions returns a list of records by Bucket name, object name and version ID, along with all the associated versions.
Retrieving records and associated metadata	● GetObject retrieves the content of the record version together with its metadata. ○ When the request includes the version ID, the specific record version is returned. ○ When the request excludes the version ID, the current (top) version is returned, unless the most recent version is a Delete Marker, in which case an error code is returned. ● HeadObject retrieves metadata about the specified record version without downloading the content of the record version.
Displaying retention controls	● GetObjectLockConfiguration retrieves the Object Lock status for the Bucket, and if Object Lock is enabled, the values for the optional Default Retention Mode and Default Retention Period. ● Additionally, the S3 GetObject and HeadObject results include: (a) Retention Mode, (b) Retain Until Date, (c) Legal Hold attribute.
Download and Transfer records and the information needed to locate the records	● GetObject downloads the specified record version and record version metadata, to a specified location. Thereafter, local capabilities may be used to transfer the record versions and associated metadata, to the regulator, in the requested format. ● When multiple versions of a record are stored, the current (top) version is returned, unless the version ID is specified in the request.

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 Object 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.[11] [emphasis added]

- The intent of paragraph (B) is:

  [R]edundancy capabilities that are designed to ensure access to Broker-Dealer Regulatory Records or the SBS Entity Regulatory Records must have a level of redundancy that is at least equal to the level that is achieved through using a backup recordkeeping system.[12] [emphasis added]

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

2.5.2 Compliance Assessment

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

2.5.3 FlashBlade Object Storage Capabilities

- For compliance with paragraph (B), FlashBlade Object 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.

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

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

- A replica of the records can be accurately regenerated from the erasure coded data segments in the event of a blade failure.

2.5.4 Additional Considerations

While FlashBlade Object Storage supports asynchronous replication to Amazon S3, this is outside the scope of this Compliance Assessment Report.

Additionally, the regulated entity is responsible for maintaining the technology, storage capacity, encryption keys, and other information and services needed to use FlashBlade Object Storage and permit access to 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 Object Storage supports the regulated entity's efforts to meet this SEC requirement for an audit system.

2.6.3 FlashBlade Object Storage Capabilities

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

- FlashBlade Object Storage immutably retains the following record attributes for the same time period as the record. These attributes provide valuable audit information related to the inputting of the record.
  - The <u>immutable</u> attributes for a record version include:
    - Unique identifier (KeyName), which is the combination of Bucket name, object name and version ID, and

        - Last modified (storage) timestamp.

- When Object Lock retention controls are applied in *Compliance* mode, the associated record content is immutably stored over its lifespan; changes to the record content are not allowed.
    - Accordingly, tracking of the inputting of changes made to the record content is not relevant to records stored with Object Lock retention controls applied in *Compliance* mode.
- In addition, management logs track each management activity performed on a Bucket, including, but not limited to Bucket creation, configuration and deletion.
    - Management logs are immutable once created.
    - Storage administrators access the management logs using the Audit Trail feature or command line interface.
- The management logs may be exported for (a) ingestion by a centralized logging server or (b) storage in a specified destination. These separate storage locations may be leveraged to retain the audit events for the same time period as the associated record.

2.6.4 Additional Considerations

In addition to relying on the immutable record metadata, the regulated entity is responsible for maintaining an audit system for inputting records and changes made to the records.

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

This section contains a summary assessment of the functionality of FlashBlade Object Storage, as described in Section 1.3, *FlashBlade Object 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.*[13] [emphasis added]

In Section 2 of this report, Cohasset assesses FlashBlade Object Storage, with Object Lock applied in *Compliance* mode, a highly restrictive option that applies integrated controls to (a) prevent modifications to the record content and certain system metadata 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 Object Storage, using Object Lock applied in *Compliance* mode. In addition, Cohasset contends that FlashBlade Object Storage, using the less restrictive *Governance* mode*,* meets these *principles-based* CFTC requirements, when the regulated entity applies appropriate procedural controls to oversee operations that may allow content to be modified or deleted prior to expiration of the retention period. The first column enumerates the CFTC regulation. The second column provides Cohasset's analysis and opinion regarding the ability of FlashBlade Object Storage, relative to these requirements.

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

CFTC 1.31(c)-(d) Regulation [emphasis added]	**Compliance Assessment Relative to CFTC 1.31(c)-(d)**
(c) Form and manner of retention. Unless specified elsewhere in the Act or Commission regulations in this chapter, all regulatory records must be created and retained by a records entity in accordance with the following requirements: *(1) Generally. Each records entity shall retain regulatory records in a form and manner that ensures the authenticity and reliability of such regulatory records in accordance with the Act and Commission regulations in this chapter.* *(2) Electronic regulatory records. Each records entity maintaining electronic regulatory records shall establish appropriate systems and controls that ensure the authenticity and reliability of electronic regulatory records, including, without limitation:* *(i) Systems that maintain the security, signature, and data as necessary to ensure the authenticity of the information contained in electronic regulatory records and to monitor compliance with the Act and Commission regulations in this chapter;*	It is Cohasset's opinion that the CFTC requirements in (c)(1) and (c)(2)(i), for records[14] with time-based retention periods, are met by the functionality of FlashBlade Object Storage, with Object Lock. The retention controls associated with Object Lock, when applied in *Compliance* mode, and the features that support the authenticity and reliability of electronic records are 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 Object Storage retains immutable metadata (e.g., Unique Identifiers and applicable creation and/or last modified timestamps) as an integral component of the records, and, therefore, these attributes are subject to the same retention controls as the associated record. These immutable attributes support both (a) records access, search and display and (b) audit system and accountability for inputting the records. Additionally, mutable metadata stored for records include Retain Until Dates (which may be extended) and Legal Hold attributes. The most recent values of mutable metadata are retained for the same time period as the associated records.
(ii) Systems that ensure the records entity is able to produce electronic regulatory records in accordance with this section, and ensure the availability of such regulatory records in the event of an emergency or other disruption of the records entity's electronic record retention systems; and	It is Cohasset's opinion that FlashBlade Object Storage capabilities to retain a persistent alternate source to reestablish the records and associated system metadata, as described in Section 2.5, *Record Redundancy*, meet the CFTC requirements (c)(2)(ii) to *ensure the availability of such regulatory records in the event of an emergency or other disruption of the records entity's electronic record retention systems.*

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

CFTC 1.31(c)-(d) Regulation [emphasis added]	**Compliance Assessment Relative to CFTC 1.31(c)-(d)**
(iii) The creation and maintenance of an up-to-date inventory that identifies and describes each system that maintains information necessary for accessing or producing electronic regulatory records.	The regulated entity is required to create and retain an *up-to-date inventory,* as required for compliance with 17 CFR § 1.31(c)(iii).
(d) Inspection and production of regulatory records. Unless specified elsewhere in the Act or Commission regulations in this chapter, a records entity, at its own expense, must produce or make accessible for inspection all regulatory records in accordance with the following requirements: *(1) Inspection. All regulatory records shall be open to inspection by any representative of the Commission or the United States Department of Justice.* *(2) Production of **paper** regulatory records. **** *(3) Production of **electronic** regulatory records.* *(i) A request from a Commission representative for electronic regulatory records will specify a reasonable form and medium in which a records entity must produce such regulatory records.* *(ii) A records entity must produce such regulatory records in the form and medium requested promptly, upon request, unless otherwise directed by the Commission representative.* *(4) Production of **original** regulatory records. ****	It is Cohasset's opinion that FlashBlade Object 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 FlashBlade Object Storage[15] in comparison to the electronic recordkeeping system requirements set forth in SEC Rules 17a-4(f)(2) and 18a-6(e)(2) and described audit system features that support the regulated entity as it meets the requirements of SEC Rules 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii).

Cohasset determined that FlashBlade Object Storage, when properly configured, has the following functionality, which meets the regulatory requirements:

- Retains the records and immutable record metadata in non-rewriteable, non-erasable format for time-based retention periods when the record versions are stored in FlashBlade Object Storage and *Compliance* mode retention controls are applied to the record.
- Permits Legal Holds to be applied to individual record versions stored in Buckets with Object Lock enabled. The Legal Hold preserves the associated records for a subpoena, legal matters or similar circumstances, and permits clearing the hold when the matter is released.
- Prohibits deletion of records until the Retain Until Date is expired and any applied Legal Hold attribute is cleared.
- Employs error correction to detect and correct bit level data errors during data transmission
- Verifies the accuracy of the recording processes, calculates and stores a checksum for each record, and uses the checksums for post-recoding validation processes.
- Provides authorized users with the capacity and tools to readily (a) query record metadata to find records, (b) list the query results, and (c) download selected records and associated metadata for a browser or other local tool to produce a human readable image and a reasonably usable electronic format.
- Maintains records redundancy to regenerate an accurate replica of the record from the erasure coded data should an error occur or an availability problem be encountered.
- Supports the regulated entity's obligation to retain an audit system for non-rewriteable, non-erasable records.

Accordingly, Cohasset concludes that FlashBlade Object 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).

[15] See Section 1.3, *FlashBlade Object 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[16] to 17 CFR § 240.17a-4 (Rule 17a-4) and 17 CFR § 240.18a-6 (Rule 18a-6), which define more technology-neutral requirements for electronic recordkeeping systems.

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

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

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

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

A.1.1 Record and Audit-Trail Alternative

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

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

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

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

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

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

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

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

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

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

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

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

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

[19] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.

[20] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.

[21] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66418.

[22] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66419.

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

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

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

> *The Commission is clarifying that a software solution that prevents the overwriting, erasing, or otherwise altering of a record during its required retention period would meet the requirements of the rule.*[24] [emphasis added]

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

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

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

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

See Section 2, *Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e),* for each SEC electronic recordkeeping system requirement and a description of the functionality of FlashBlade Object 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).[26]

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

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

[23] 2003 Interpretative Release, 68 FR 25282.

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

[25] 2003 Interpretative Release, 68 FR 25283.

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

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

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

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

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

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

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

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

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

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

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.

©2024 Cohasset Associates, Inc.

This Compliance Assessment Report and the information contained herein are copyrighted and the sole property of Cohasset Associates, Inc. Selective references to the information and text of this Compliance Assessment Report are permitted, provided such references have appropriate attributions and citations. Permission is granted for in-office reproduction so long as the contents are not edited and the look and feel of the original is retained.