Cohasset Associates

IBM® Storage Ceph®

COMPLIANCE ASSESSMENT

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

Abstract

IBM® Storage Ceph® is an open source, scalable and software defined multi-protocol object storage solution designed for enterprise clients. IBM Storage Ceph offers an *Object Lock* feature, which was 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 IBM Storage Ceph (see Section 1.3, *IBM Storage Ceph 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).

Cohasset asserts that IBM Storage Ceph, when properly configured and used with *Object Lock,* 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 IBM Storage Ceph 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.

October 2023

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

+1.312.527.1550 | www.cohasset.com

Table of Contents

Abstract **1**

Table of Contents **2**

1 • Introduction **3**

1.1 Overview of the Regulatory Requirements 3

1.2 Purpose and Approach 4

1.3 IBM Storage Ceph Overview and Assessment Scope 5

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

2.1 Record and Audit-Trail 6

2.2 Non-Rewriteable, Non-Erasable Record Format 7

2.3 Record Storage Verification 16

2.4 Capacity to Download and Transfer Records and Location Information 17

2.5 Record Redundancy 18

2.6 Audit System 20

3 • Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d) **22**

4 • Conclusions **25**

Appendix A • Overview of Relevant Electronic Records Requirements **26**

A.1 Overview of SEC Rules 17a-4(f) and 18a-6(e) *Electronic Recordkeeping System* Requirements 26

A.2 Overview of FINRA Rule 4511(c) *Electronic Recordkeeping System* Requirements 28

A.3 Overview of CFTC Rule 1.31(c)-(d) *Electronic Regulatory Records* Requirements 29

About Cohasset Associates, Inc. **30**

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 IBM Storage Ceph 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 IBM Storage Ceph for preserving required electronic records, IBM® 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.

IBM engaged Cohasset to:

- Assess the functionality of IBM Storage Ceph, 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 IBM Storage Ceph; 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 IBM Storage Ceph and its functionality or other IBM 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 IBM 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 IBM Storage Ceph Overview and Assessment Scope

1.3.1 IBM Storage Ceph Overview

The IBM® Storage Ceph® is an open source, scalable and software defined multi-protocol object storage solution designed for enterprise clients that stores records[4] in buckets on object storage devices (OSDs).

The IBM Storage Ceph storage architecture is depicted in the Figure 1:

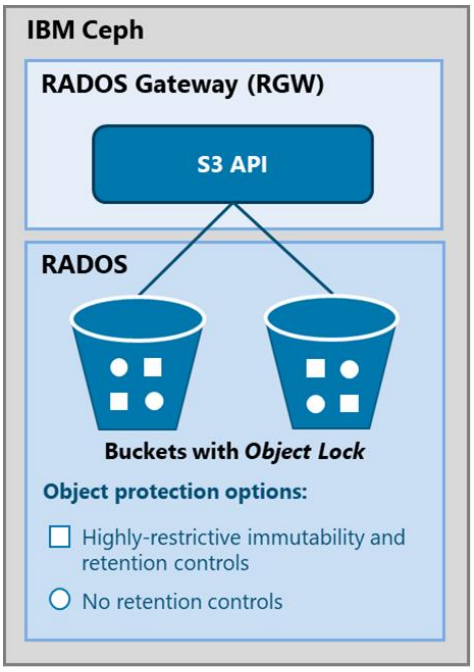

Figure 1: IBM Ceph logical storage architecture

- **RADOS Gateway (RGW)** natively supports Amazon S3 APIs (application programming interface), which can be used for data management, collaboration and archiving.
- **RADOS** (**R**eliable **A**utonomic **D**istributed **O**bject **S**torage) provides low-level data object storage and manages all replication, erasure coding, placement, rebalancing, and repair.
- **Buckets** used to store objects or object versions (if versioning is enabled for the Bucket). For Buckets intended to retain required records in compliance with SEC Rules 17a-4(f) and 18a-6(e), the *Object Lock* feature and versioning must be enabled for the Bucket.
  - *Object Lock* retention controls must be applied to each required record version and may be set in either highly-restrictive *Compliance* mode or less-restrictive *Governance* mode. Note: When the less-restrictive *Governance* mode controls are applied, procedural controls and monitoring are required to scrutinize actions taken to shorten or remove retention controls and prematurely delete required records.
  - Additionally, the *Legal Hold* attribute (Y/N) may be separately applied to record versions.

1.3.2 Assessment Scope

For this SEC requirement to preserve electronic records in a non-rewriteable, non-erasable record format for the required retention period, Cohasset assesses the *Object Lock* configured with the highly-restrictive *Compliance* or less-restrictive *Governance* mode.

This report assesses IBM Storage Ceph Release 7.0 when properly configured and deployed on-premises, using hardware certified for RHEL (Red Hat Enterprise Linux) usage. Other deployments are excluded from this assessment.

NOTE: Software as a Service (SaaS) and Platform as a Service (PaaS) solutions using the IBM Storage Ceph, when IBM or a third party manages or provides the solution to a regulated entity, are 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 typically uses the term *record* (versus data, file, version, or object) 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 IBM Storage Ceph, 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 IBM Storage Ceph
- ***IBM Storage Ceph 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 IBM Storage Ceph, as described in Section 1.3, *IBM Storage Ceph 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 IBM Storage Ceph 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 IBM Storage Ceph, 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 2019 interpretation further refined the 2003 interpretation. In particular, it noted that the 2003 interpretation described*

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

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

> *a process of integrated software and hardware codes and clarified that "a software solution that prevents the overwriting, erasing, or otherwise altering of a record during its required retention period would meet the requirements of the rule."*
> *****
> *In 2001, the Commission issued guidance that Rule 17a-4(f) was consistent with the ESIGN Act. The final amendments to Rule 17a-4(f) do not alter the rule in a way that would change this guidance.*[7] [emphasis added]

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

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

2.2.2 Compliance Assessment

Cohasset asserts that the functionality of IBM Storage Ceph, with *Object Lock* applied to records in either highly restrictive *Compliance* mode or less-restrictive *Governance* 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.

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

2.2.3 IBM Storage Ceph Capabilities

This section describes the functionality of IBM Storage Ceph 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

- Records are transmitted to IBM Storage Ceph (via the S3 compatible restful API provided by the RADOS Gateway service commands) and are stored in Buckets.
- Buckets intended to store required records must have both (a) the *Object Lock* feature enabled and (b) versioning enabled, to allow each record *version* to be retained as a separate record with its own retention controls. Optionally, the Bucket may be configured with a pair of *Default Retention* control values: *Default Object Lock mode* and *Default Retention Period*.

---

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.

- Retention controls are applied to records, by either (a) transmitting explicit *Object Lock* mode and *Retain Until Date* attributes, when storing a new record or applying the retention controls to a previously stored record or (b) configuring *Default Retention* values for the Bucket where the record is stored.
- The following table summarizes the retention controls applied to records by *Object Lock,* in *Compliance* versus *Governance* modes.

	***Object lock,* in highly-restrictive *Compliance* mode**	***Object lock,* in less-restrictive *Governance* mode**
Protecting record content and immutable metadata	• Versioning protects the record content and associated system metadata for its lifespan. Any attempt to modify or overwrite results in storing a new version, with separate retention controls. • Renaming Buckets, objects, and version identifiers is prohibited.	
Restricting changes to retention controls	• The *Object Lock* feature applied to a Bucket cannot be removed. • The *Object Lock* retention controls applied to a record (i.e., an object version) cannot be downgraded to *Governance* mode or removed. Accordingly, *Compliance* mode assures retention controls are not circumvented by any user or process. • The *Retain Until Date* applied to a record (i.e., an object version) may be extended at any time, though it cannot be reduced or removed.	• The *Object Lock* feature applied to a Bucket cannot be removed. • The *Object Lock* retention controls applied to a record (i.e., an object version) can be upgraded to highly-restrictive *Compliance* mode and the *Retain Until Date* applied to a record can be extended, at any time. • Administrators with *BypassGovernanceRetention* privileges can: ○ Remove the *Object Lock* retention controls applied to a record, ○ Reduce or remove the *Retain Until Date* applied to a record. Accordingly, procedural controls and monitoring are required to scrutinize administrator actions taken to bypass or remove retention controls. • Note: The *Object Lock* mode and *Retain Until Date* are a pair and both must be removed to clear retention controls.
Applying and removing legal holds	• The record version's *Legal Hold* attribute may be set (Yes) or cleared (No) at any time and may be applied to versions without applied retention controls.	
Restricting deletion of Buckets and records	• The Bucket cannot be deleted unless it is empty. • Deletion of each record version (i.e., an object version) and its associated immutable metadata are prohibited until the applied *Retain Until Date* expires and the *Legal Hold* attribute is clear (No). Accordingly, *Compliance* mode assures retention controls cannot be circumvented by any user or process. • Deletion of the record (without identifying the Version) appends a Delete Marker as the current (top) version and all other existing record versions are hidden but remain unmodified. The Delete Marker may be removed to reinstate the original record versions.	• The Bucket cannot be deleted unless it is empty • Administrators with *BypassGovernanceRetention* privileges can delete a record version (i.e., an object version) and its associated immutable metadata before the applied *Retain Until Date* expires and the *Legal Hold* is removed (No). Accordingly, procedural controls and monitoring are required to scrutinize administrator actions taken to bypass or remove retention controls. • Deletion of the record (without identifying the Version) appends a Delete Marker, as the current (top) version and all other existing record versions are hidden but remain unmodified. The Delete Marker may be removed to reinstate the original record versions.

2.2.3.2 Bucket and Identity and Access Management Configurations

- In IBM Storage Ceph, Buckets are logical containers that store records.
  - Each Bucket name must be unique within a Namespace and cannot be changed, after Bucket creation.
- Records are stored within each Bucket, in a flat storage hierarchy.
  - Each record version (i.e., object version) is assigned separate retention controls.
  - 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 and Identity and Access Management (IAM) configurations related to the *Object Lock* features.

	Bucket and IAM Configurations related to *Object Lock* features
***Object Lock* feature**	• For each Bucket intended to retain records in compliance with SEC Rules 17a-4(f) and 18a-6(e), the *Object Lock* feature may be enabled during initial Bucket creation or anytime thereafter. When enabling *Object Lock* after bucket creation, existing objects will require explicit retention to be applied for compliance with the Rules. • Once the *Object Lock* feature is enabled for a Bucket, it cannot be suspended, disabled or removed.
Versioning	• Versioning must be enabled (On) and must remain enabled. ○ When *Object Lock* is enabled after Bucket creation, the user must first enable versioning. • Each record version is separately managed, with separate retention and legal hold controls. When controls are set without specifying a version, the controls apply to the current (top) version.
***Default retention* values**	• Optionally, Default Retention values (i.e., *Default Object Lock Mode* and *Default Retention Period*) may be configured for a Bucket as a pair; requiring both or neither to be set. ○ The *Default Object Lock Mode* may be set to either *Compliance mode* (highly-restrictive) or *Governance mode* (less-restrictive). (See Section 2.2.3.3, *Records and Retention Controls*, for details regarding retention controls associated with each mode.) ○ The *Default Retention Period* may be specified in terms of days. The allowable range is between 1 and 24,820 days (68 years). The *Default Retention Period* is added to the record's creation/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 retention controls are not transmitted with the record version. See Section 2.2.3.3, *Records and Retention Controls*. ○ Setting these defaults during Bucket creation assures retention controls are applied to all record versions in the Bucket. ○ Setting or modifying these defaults on existing Buckets will not automatically apply or update retention controls on existing records. Instead, explicit retention controls must be transmitted and applied to the existing records. • 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.
IAM Policies	• Identity and Access Management (IAM) roles define a set of privileges that grant access to actions and resources in IBM Storage Ceph. The IAM Role is applied to S3/RGW users (e.g., source systems) permissioned to store records in the Bucket. • Note: If the user has not been granted the prerequisite privileges, the action will fail.

2.2.3.3 Records and Retention Controls

- Each version of an object is considered a separate record and is comprised of:
  - The complete content of the record (object), which is unmodifiable.
  - *Immutable* attributes, including unique object KeyName (which includes Bucket Name and Object Name), Version ID, creation/storage timestamp (mdate), object size, and user-defined custom attributes (key-value pairs).
  - *Mutable* attributes, which includes *Retain Until Date*, *Object Lock* mode[10], access control lists (ACLs), and user-defined tags.
- Retention controls 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 controls (*Object Lock* mode and the *Retain Until Date*) applied during the storage process, based on (a) the retention attributes transmitted with the record version (columns with orange highlighted headings) and (b) the *Object Lock* default values configured for the Bucket (columns with blue highlighted headings).

Transmitted Object Lock Mode	Transmitted Retain Until Date	Record Version's Retention Controls if Bucket has no default retention settings	Record Version's Retention Controls if Bucket has default retention settings
Null	mm/dd/yyyy	• Error returned, write operation fails	
Null	Null	• Record version is stored **without** retention controls	• Record version is set to the Bucket's *Default Retention* mode (*Compliance* or *Governance*) and *Retain Until Date* is record version's creation/storage date + Bucket's ***Default*** *Retention period*
Governance	mm/dd/yyyy	• Record version is set to *Governance* mode and *Retain Until Date* is mm/dd/yyyy	
Governance	Null	• Error returned, write operation fails	
Compliance	mm/dd/yyyy	• Record version is set to *Compliance* mode and retain until day is mm/dd/yyyy	
Compliance	Null	• Error returned, write operation fails	

- The preceding table explains the retention controls applied during record creation/storage. In addition, retention controls may be applied to existing records, as described in the following table, in the row labeled *Modifying or removing retention controls*.
- The following table describes the integrated retention controls applied by *Object Lock* features.

[10] An *Object Lock* mode set to *Compliance* cannot be changed to *Governance* mode or cleared by any user.

	***Object Lock,* in highly-restrictive *Compliance* mode**	***Object Lock,* in less-restrictive *Governance* mode**
Managing versions	● Versioning must be enabled for the Bucket. When enabled, each version of an object is considered a separate record and must have its own applied *Object Lock* mode, *Retain Until Date*, and *Legal Hold* attribute (optional). ○ If an object is uploaded with an object KeyName that already exists in the Bucket, a new record version, with a new Version ID, is automatically created. ○ If custom attributes (key value pairs) are added or modified for a record, a new record version is automatically created. ○ If the *Object Lock* mode, *Retain Until Date*, *Legal Hold* attribute, ACLs, or user-defined S3 tags are added or modified for a record, updates are stored without creating a new record version.	
Protecting record content and metadata	● Each record version, together with its *immutable attributes* (metadata), is immutably stored for its lifespan. ○ All attempts to **modify** the contents of a record version, during its lifespan, are rejected. ○ All attempts to change unique object KeyName are rejected. Additionally, version identifiers are system-generated and are immutable. ● All attempts to **overwrite** an existing record, results in storing a new version, with separately applied retention controls and *Legal Hold* attribute (if applicable). ● After retention controls expire and any legal hold is removed, the record version may be deleted, but cannot be modified or overwritten.	
Modifying or removing retention controls	● For record versions previously set to *Compliance* mode, authorized users: ○ Cannot change *Compliance* to *Governance.* ○ Can extend, but cannot reduce, the *Retain Until Date*. ○ Cannot remove retention controls (i.e., cannot change from *Compliance* to *Null* and cannot remove the *Retain Until Date).*	● For record versions previously set to *Governance* mode, authorized users: ○ Can change *Governance* to *Compliance.* ○ Can extend or reduce the *Retain Until Date*. ○ Can remove retention controls (i.e., can change from *Governance* to *Null* and remove the *Retain Until Date*). Note: Only users with *BypassGovernanceRetention* permission may shorten the *Retain Until Date* or remove retention controls.
	● If the Version ID is explicitly identified, the updated retention attributes apply to the explicit record version. ● If the Version ID is not explicitly identified, the updated retention attributes apply to the current (top) record version. ● Changes to the retention attributes do not generate a new version and do not affect the record version's creation/storage (last modified) date. ● The *Retention Mode* and *Retain Until Date* must be submitted as a pair. If only one attribute is transmitted, the operation fails.	
Modifying Legal Hold attribute	● A record version's *Legal Hold* attribute may be set (Yes) or cleared (No), regardless of applied retention controls. See Section 2.2.3.4, *Legal Holds (Temporary Holds),* for additional information.	
Restricting deletion	● A specific record version may be deleted when both the *Retain Until Date* is expired (is in the past) and the *Legal Hold* attribute is clear (No). Otherwise, deletion is rejected. ● No users are allowed to shorten or remove the *Retain Until Date* or delete an unexpired record version.	● A specific record version may be deleted when both the *Retain Until Date* is expired and the *Legal Hold* attribute is removed (No). ● Additionally, users with *BypassGovernanceRetention* permission may shorten the *Retain Until Date*, remove retention controls or delete unexpired record versions.
	● Deleting a record, without specifying a Version ID, appends a Delete Marker as the current (top) version, which hides the record. Removing the Delete Marker reinstates the record. See Section 2.2.3.5, *Deletion Controls,* for additional information.	

	***Object Lock*, in highly-restrictive *Compliance* mode**	***Object Lock*, in less-restrictive *Governance* mode**
Copying records	● A record may be **copied** to a different Bucket. ○ The creation/storage timestamp of the copy reflects the date and time that the copy is stored in the destination Bucket (not the date and time 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.	
Changing permissions	● Access control lists (ACLs) may be modified.	

► Additionally, Buckets, with the *Object Lock* feature enabled, are protected:

- All attempts to change a Bucket name are rejected.
- The Bucket cannot be moved, unless it is empty.
- The Bucket cannot be deleted, unless it is empty.

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.

► The following table separately describes the legal hold features for Buckets configured with *Object Lock* enabled.

	Legal Holds and related to *Object Lock* features
Applying and removing legal holds	● Using RGW, 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 *Retain Until Date* and *Object Lock* mode; 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. ● The *Legal Hold* attribute is automatically replicated, when placement groups are configured to store a full set of records on two object storage devices (OSDs).
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 cleared (No). ● When the *Legal Hold* attribute is cleared (No), this attribute no longer mandates preservation of the record version; however other retention controls continue to be enforced for the record version.
Displaying legal holds	● The *Legal Hold* attribute applied to a record version is displayed with the GET (list) Object Legal Hold operation.
Retention change restrictions	● *Legal Hold* attribute does not impact allowed changes to the *Object Lock* mode and *Retain Until Date*. For example, the record version's *Retain Until Date* may be extended while subject to a legal hold.

2.2.3.5 Deletion Controls

- 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.

	***Object Lock*, in highly-restrictive *Compliance* mode**	***Object Lock*, in less-restrictive *Governance* mode**
Deleting records (without specifying VersionID)	• When the Version ID is not specified, actions to delete a record (regardless of the status of the retention controls), appends a Delete Marker as the current (top) version. ○ Delete markers can be removed, which results in reinstating or recovering the deleted (hidden) record.	
Deleting specific record version	• Deleting a specific record version is completed only when both the *Retain Until Date* is expired and *Legal Hold* attribute is clear (No). Otherwise, deletion is rejected.	
	• Privileged delete (i.e., *BypassGovernanceRetention*) cannot be used to prematurely delete record versions.	• Users with *BypassGovernanceRetention* permission may shorten the *Retain Until Date*, remove retention controls or delete unexpired records, by identifying the specific record version.
Using a Lifecycle Policy for deletion	• A Lifecycle Policy may be configured to automatically delete eligible records.	• A Lifecycle Policy may be configured to automatically delete eligible records. • The *BypassGovernanceRetention* override cannot be utilized with a Lifecycle Policy.
Deleting Buckets	• The Bucket, with *Object Lock* enabled, cannot be deleted, unless it is empty. Accordingly, deleting a Bucket to effectuate the premature deletion of records is prohibited.	

2.2.3.6 Security

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

- Role-Based Access Control security and identity and access management policies provide the means to create, delete, and maintain accounts and control user permissions.
- Encryption options for records and metadata include:
  - Implementation of cluster-wide, at-rest, or user-managed inline object encryption; operator-managed encryption keys and user managed encryption keys are supported.
  - FIPS 140-2 support when running on certified Red Hat Enterprise Linux versions.
- Key management service integration is supported for Hashicorp Vault, IBM Security Guardium Key Lifecycle Manager (SGKLM), and OpenStack Barbican. External key management service is compatible with any KMIP-compliant key management infrastructure.
- Authentication and authorization is integrated with Microsoft Active Directory, lightweight directory access protocol (LDAP), AWS Auth v4, Secure Token Service using OIDC or Oauth2 Single Sign On and KeyStone v3.
- Optionally, the administrator may enable Multi-Factor Authentication, which requires users to enter a one-time password, when removing eligible objects on the configured Bucket.

2.2.3.7 Clock Management

To meet the requirements of the Rule, Cohasset asserts that every system clock must synchronize to an external time server, e.g., a network time protocol (NTP) clock.

- The IBM Storage Ceph enforces enabling NTP during system configuration and regularly checks the time of the external source (NTP) and resynchronize time.
  - If time drift is detected during a health check, a warning is presented in the dashboard and an alert is sent to the client. Chronyd will adjust system time to synchronize with the NTP clock.

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 Versioning on the Buckets intended to store required records.
- Applying retention controls, which meet regulators' retention requirements, to each record (i.e., each record version). For Buckets that storing records required for compliance with the Rules, Cohasset recommends configuring (a) an appropriate *Default Retention Period* and (b) *Default Object Lock* mode of *Compliance,* to assure highly-restrictive retention controls are applied to all records stored in the Bucket.
- Establishing procedural controls and monitoring to scrutinize administrator actions taken to bypass retention controls, if less-restrictive *Governance* mode retention controls will be applied.
- Ensuring all records required for compliance with the Rules are successfully stored with retention controls, preferably within 24 hours of creation.
- Setting *Legal Hold* attributes to Yes, as needed, to preserve records for legal matters, government investigations, external audits and other similar circumstances; and, setting the *Legal Hold* attribute to 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.
- Storing records requiring event-based[11] retention periods in a separate compliant system, since IBM Storage Ceph does not currently support event-based retention periods.
- Appropriately assigning permissions required to manage the retention controls and properly configuring the roles and Buckets that will retain required records.
- Setting appropriate security controls to (a) restrict network ports and protocol access, (b) establish roles-based access, and (c) encrypt data in transit and while at rest.
- Ensuring that NTP clock servers are appropriately configured and monitored.

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

[11] 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 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 IBM Storage Ceph meets this SEC requirement for complete and accurate recording of records and post-recording verification processes when the considerations identified in Section 2.3.4 are satisfied.

2.3.3 IBM Storage Ceph Capabilities

The recording and post-recording verification processes of IBM Storage Ceph are described below.

2.3.3.1 Recording Process

- Optionally, an MD5 checksum may be transmitted with the record object. When transmitted, the record object will be stored only if the MD5 checksum value calculated by IBM Storage Ceph matches the uploaded checksum. If it does not match, an error is reported, and the record object must be re-uploaded.
- IBM Storage Ceph utilizes advanced electronic recording technology which applies a combination of checks and balances to assure that records are written in a high quality and accurate manner.

2.3.3.2 Post-Recording Verification Process

- IBM Storage Ceph uses erasure coding to divide the record into strips of data blocks and calculates parity. The integrity of the record is maintained by leveraging the parity to calculate any missing data blocks.
- IBM Storage Ceph employs a background healing process that scans the data blocks of a record for checking and correcting errors. If a data block is corrupt, an automatic recovery process is initiated to rebuild the data block from the other valid data and parity blocks.
- During retrieval, checksums are used to confirm record integrity and ensure that an accurate record is delivered.

2.3.4 Additional Considerations

- The source system is responsible for transmitting the complete contents of the required records, and Cohasset recommends:
  - The source system send a checksum for IBM Storage Ceph to confirm the complete and accurate transmission, when inputting records.

- Using HTTPS encryption protocol, Transport Layer Security (TLS), to encrypt communications when practical, to reduce the chance of network-level errors when transmitting and inputting the records.

- For retrieval, Cohasset recommends that the source system request transmission of a checksum with the record, for validation of the transmission.

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 IBM Storage Ceph meets this SEC requirement to maintain the capacity to readily download and transfer the records and the information used to locate the records when the considerations described in Section 2.4.4 are satisfied.

2.4.3 IBM Storage Ceph Capabilities

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

- When each record is written, IBM Storage Ceph systematically generates and stores a unique KeyName (which includes Bucket Name and Object name), Version ID, and the creation/storage timestamp (mdate). These attributes are immutably retained for the lifespan of the record and facilitate findability.
- IBM Ceph assures that hardware and software capacity allows for ready access to the records and metadata attributes.
  - Using the RGW or CLI (command line interface), authorized users can:
    - View retention controls and legal hold attributes via the S3 API or S3 Client to call the *GetObjectLockConfiguration* command.

- List records in a Bucket, using either of the following commands:
  - *ListObject*: Returns a list of the records, by KeyName; if the most recent version is a Delete Marker the record object is not returned in the list.
  - *ListObjectVersions*: Returns a list of records by KeyName, along with all the associated versions.
- Retrieve records in a bucket, using the GetObject command:
  - When the request includes the Version ID, the specific record version is returned.
  - When the request excludes the Version ID, the most recent version is returned, unless the most recent version is a Delete Marker, in which case an error code is returned.
- Download selected record objects and the associated metadata (index) attributes to a designated storage location. When multiple versions of a record are stored, the top-level version is returned, by default. The specific Version ID must be specified in the search and download requests.

2.4.4 Additional Considerations

Additionally, the regulated entity is responsible for: (a) authorizing user privileges, (b) maintaining appropriate technology and resource capacity, encryption keys, and other information and services needed to use IBM Storage Ceph 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.[12] [emphasis added]

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

- The intent of paragraph (B) is:

  [R]edundancy capabilities that are designed to ensure access to Broker-Dealer Regulatory Records or the SBS Entity Regulatory Records must have a level of redundancy that is at least equal to the level that is achieved through using a backup recordkeeping system.[13] [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 IBM Storage Ceph meets both paragraphs (A) and (B) of this SEC requirement by retaining a persistent duplicate copy of the records or alternate source to reestablish the records, when (a) properly configured as described in Section 2.5.3 and (b) the considerations described in Section 2.5.4 are satisfied.

2.5.3 IBM Storage Ceph Capabilities

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

2.5.3.1 Redundant Set of Records

- For compliance with paragraph (A), to maintain a redundant set of records, IBM Storage Ceph uses replication schemas. IBM Storage Ceph has two different schemas available to choose from:
  - Replication Schema: Uses placement groups which aggregates and stores a full set of records on two or more object storage devices (OSDs).
  - Erasure Coding Schema: Stores data blocks of records redundantly across pools. In the event of a disk or node failure, the original record can be regenerated from the data blocks.
- Further, IBM Ceph can be configured to use multisite asynchronous replication to another Ceph cluster in a different region. When enabling this feature, both sites are exact replicas of each other, including retention controls and metadata.

2.5.3.2 Other Redundancy Capabilities

- For compliance with paragraph (B), IBM Storage Ceph uses erasure coding to store data blocks of records redundantly across pools. In the event of a disk or node failure, the original record can be regenerated.

2.5.4 Additional Considerations

In addition, for this requirement, the regulated entity is responsible for: (a) maintaining the technology, storage capacity, encryption keys, and other information and services needed to use IBM Storage Ceph and permit access to the redundant records.

[13] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66421.

2.6 Audit System

2.6.1 Compliance Requirement

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

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

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

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

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

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

2.6.2 Compliance Assessment

Cohasset asserts that IBM Storage Ceph, in conjunction with audit event logging features, when configured, supports the regulated entity's efforts to meet this SEC requirement for an audit system.

2.6.3 IBM Storage Ceph Capabilities

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

- When inputting records, IBM Storage Ceph (a) systematically generates a unique KeyName (which includes Bucket Name and Object name), (b) Version ID and (c) creation/storage timestamp (mdate), which is assigned when the record is written. These attributes are immutable, and chronologically account for each inputted record and are retained for the same time period as the record.
- Each record and its immutable metadata is immutably stored over its lifespan; therefore, no changes are allowed once the record is stored. Accordingly, tracking of record changes is not relevant to IBM Storage Ceph.
- addition to the immutable record metadata, the OPS log may be enabled to capture record operations, which includes Bucket, time, user, RGW commands, status, errors, and other configurable values.
  - The OPS logs may be exported for ingestion by a centralized logging server or output to be stored on a specified destination. These separate storage locations may be leveraged to retain the audit events for the same time period as the associated record.
- Optionally, IBM Storage Ceph may be configured to use either Syslog or StdOut for system operations to capture records related audit events. These logs write to the configured location for storage.

2.6.4 Additional Considerations

The regulated entity is responsible for maintaining an audit system for inputting records and for keeping the audit events for the same time period as the associated record. In addition to relying on the immutable metadata, the regulated entity may utilize the OPS Log alone or in conjunction with another system.

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

This section contains a summary assessment of the functionality of IBM Storage Ceph, as described in Section 1.3, *IBM Storage Ceph 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.*[14] [emphasis added]

In Section 2 of this report, Cohasset assesses IBM Storage Ceph, with *Object Lock,* set to: (1) *Compliance* mode, a highly-restrictive option, which provides both overwrite protection and strict retention controls and (2) *Governance* mode*,* a less-restrictive option, which provides overwrite protection but requires administrative procedures and monitoring to ensure compliant retention, since authorized administrators are allowed to shorten or remove retention controls. See subsection 2.2.3.1, *Overview*, for a summary of controls for *Object Lock in Compliance mode* and *Object Lock in Governance mode* options.

In the following table, Cohasset correlates the functionality of IBM Storage Ceph, when configured to meet SEC requirements, with the *principles-based* CFTC requirements related to the *form and manner of retention* and the *inspection and production of regulatory records*. The first column enumerates the CFTC regulation. The second column provides Cohasset's analysis and opinion regarding the ability of IBM Storage Ceph to meet the requirements for electronic regulatory records in CFTC Rule 1.31(c)-(d).

[14] 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;*	Cohasset asserts that the CFTC requirements in (c)(1) and (c)(2)(i), for records[15] with time-based retention periods, are met by the functionality of IBM Storage Ceph, with *Object Lock,* when in *Compliance* mode or *Governance* mode. The functionality that supports retention, 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] IBM Storage Ceph retains immutable metadata attributes (e.g., Unique Identifiers and creation/storage timestamp) as an integral component of the records, and, therefore, these attributes are subject to the same retention controls as the associated record. These immutable attributes support both (a) records access, search and display and (b) audit system and accountability for inputting the records. Additionally, mutable metadata attributes stored for records include retention controls and *Legal Hold* attributes. The most recent values of mutable metadata are retained for the same time period as the associated records. Further, IBM Storage Ceph in conjunction with the audit event logging features (i.e., Syslog, StdOut and OPS Log), when enabled, tracks audit events and provides storage options for retaining this additional audit system information for the same time period as the record. For additional information, see Section 2.6, *Audit System*.

[15] 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	Cohasset upholds that IBM Storage Ceph capabilities described in Section 2.5, *Record Redundancy*, including methods for a persistent duplicate copy or alternate source to reestablish the records and associated system metadata, meet the CFTC requirements (c)(2)(ii) to *ensure the availability of such regulatory records in the event of an emergency or other disruption of the records entity's electronic record retention systems*.
(iii) The creation and maintenance of an up-to-date inventory that identifies and describes each system that maintains information necessary for accessing or producing electronic regulatory records.	The regulated entity is required to create and retain an *up-to-date inventory,* as required for compliance with 17 CFR § 1.31(c)(iii).
(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. ****	Cohasset affirms that IBM Storage Ceph 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 IBM Storage Ceph[16] 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 IBM Storage Ceph, 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 by applying *Object Lock,* in *Compliance* or *Governance* modes. Note: When the less-restrictive *Governance* mode controls are applied, procedural controls and monitoring are required to scrutinize use of *BypassGovernanceRetention* to shorten or remove retention controls and prematurely delete required records.
- Applies *Legal Holds* to immutably preserve records for a subpoena, legal hold or similar circumstances, and permits clearing the hold when the matter is released.
- Prohibits deletion of records until the *Retain Until Date* has expired and any applied legal hold has been cleared. Note: When *Governance* mode controls are applied, monitoring is required to scrutinize use of *BypassGovernanceRetention* to prematurely delete required records.
- Verifies the accuracy of the process for storing and retaining records, utilizing a checksum (MD5 Hash), which is received from the source system during the recording process and is stored as a metadata attribute and utilized for post-recording verification.
- Provides authorized users with the capacity and tools to readily (a) query record metadata to find records, (b) list the query results, and (c) download selected records and associated metadata attributes for a browser or other local tool to produce a human readable image and a reasonably usable electronic format.
- Maintains records redundancy to either (a) retrieve an accurate replica of the record from a persistent duplicate copy or (b) 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 IBM Storage Ceph, 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).

[16] See Section 1.3, *IBM Storage Ceph 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[17] 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.*[18] [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.*[19] [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.

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

[18] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66428.

[19] 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.*[20] [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.*[21] [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."*[22] [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****[23] [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).

[20] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.
[21] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.
[22] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66418.
[23] 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.*[24] [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.*[25] [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.*[26] [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 IBM Storage Ceph 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).[27]

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.*

---

24 2003 Interpretative Release, 68 FR 25282.

25 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).

26 2003 Interpretative Release, 68 FR 25283.

27 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.*[28] [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 IBM Storage Ceph in relation to each requirement, see Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*.

[28] 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.