Cohasset Associates

SEC 17a-4(f) & CFTC 1.31(c)-(d) Compliance Assessment

IBM Cloud Object Storage

Abstract

IBM Cloud Object Storage ("COS") is a private cloud based architecture for storing and accessing record objects. The IBM COS vault with retention enabled, in combination with other IBM COS capabilities, are designed to meet securities industry requirements for preserving record objects in a non-rewriteable and non-erasable format, by protecting each record object from being overwritten or erased until it has been stored for the applied retention period and legal holds.

In this Assessment Report, Cohasset Associates, Inc. ("Cohasset") assesses the capabilities of the IBM COS vault with retention enabled relative to the electronic records recording, storage and retention requirements of the:

- Securities and Exchange Commission (SEC) in 17 CFR § 240.17a-4(f), which regulates exchange members, brokers or dealers.
- Financial Industry Regulatory Authority (FINRA) Rule 4511(c).
- Commodity Futures Trading Commission (CFTC) in regulation 17 CFR § 1.31(c)-(d), which regulates commodity futures trading.

It is Cohasset's opinion that the IBM COS vault with retention enabled, Release 3.12.0, when properly configured to store and retain *time-based* records in non-erasable and non-rewriteable format, meets the relevant storage requirements of SEC Rule 17a-4(f) and FINRA Rule 4511, which defer to SEC Rule 17a-4. It also meets the requirements of CFTC Rule 1.31(c)-(d) for the information stored on the solution.

See Section 2 for Cohasset's detailed assessment of SEC requirements, Section 3 for a summary assessment of CFTC requirements, Section 4 for conclusions, and Section 5 for an overview of the relevant Rules.

BENEFIT FROM COHASSET'S INDUSTRY INSIGHT AND EXPERIENCE

Core to Cohasset's practice is its delivery of records management and information governance professional consulting services, education and training. Cohasset's expert consulting services are tailored to support a multitude of regulated organizations, including those in the financial services industry. Cohasset serves both domestic and multi-national clients, aligning information lifecycle controls with their organizations' business priorities and facilitating regulatory compliance and risk mitigation, all the while generating measurable business efficiencies.

Cohasset has assessed the spectrum of storage technologies and systems designed to meet the requirements of the Securities and Exchange Commission (SEC) Rule 17a-4(f), (the "Rule"), as defined by 1) the No Action Letter in 1993 (allowing broker dealers to use non-erasable, non-rewriteable digital storage media); 2) the issuance of the Rule in 1997; and 3) the Interpretive Release in 2003, which authorizes the use of erasable storage, conditioned on integrated control codes, to prevent premature deletion of records.

Table of Contents

1 | Introduction

The Securities and Exchange Commission (SEC) defines rigorous and explicit requirements for regulated entities[1] that elect to retain books and records on electronic storage media. Additionally, effective August 28, 2017, the CFTC promulgated new principles-based requirements on the form and manner in which regulated entities retain and produce books and records, including provisions for electronic regulatory records.

Given the prevalence of electronic retention of books and records, these requirements apply to most broker-dealer and commodity futures trading firms and other organizations with similarly regulated operations.

The IBM Cloud Object Storage vault with retention enabled was designed to support compliance with these stringent electronic records requirements for the recording, storage and retention of regulated books and records. To evaluate its compliance with SEC Rule 17a-4(f) and CFTC Rule 1.31(c)-(d), IBM engaged Cohasset to complete an independent and objective assessment of the capabilities of the IBM Cloud Object Storage vault with retention enabled relative to these requirements.

This Introduction *briefly summarizes the regulatory environment, explains the purpose and approach for Cohasset's assessment, and provides an overview of IBM Cloud Object Storage.*

1.1 Overview of the Regulatory Requirements

1.1.1 SEC Rule 17a-4(f) Requirements

In 17 CFR §§ 240.17a-3 and 240.17a-4, the SEC stipulates recordkeeping requirements, including retention periods, for the securities broker-dealer industry. On February 12, 1997, the SEC adopted amendments to 17 CFR § 240.17a-4 (the "Rule" or "SEC Rule 17a-4"). These amendments to paragraph (f) expressly allow books and records[2] to be retained on electronic storage media, subject to explicit standards.

> *The Commission is adopting a rule today which, instead of specifying the type of storage technology that may be used, sets forth standards that the electronic storage media must satisfy to be considered an acceptable method of storage under Rule 17a–4. [emphasis added]*

Further, the SEC issued two Interpretive Releases (No. 34-44238 on May 1, 2001, and No. 34-47806 on May 7, 2003), which pertain specifically to the electronic storage media requirements of paragraph (f) of the Rule. This Assessment Report includes a summary of the current Rule and these two Interpretive Releases in Section 5.1, *Overview of SEC Rule 17a-4(f) Electronic Storage Requirements*.

---

[1] Throughout this report, Cohasset uses the phrase "*regulated entity*" to refer to organizations required to retain records in accordance with the media requirements of the SEC, FINRA or the CFTC. Accordingly, Cohasset uses "*regulated entity*" instead of "*records entity*," which the CFTC has defined as "any person required by the Act or Commission regulations in this chapter to keep regulatory records."

[2] Regulators use the phrase "*books and records"* to describe information about certain business transactions, customers, personnel and other administrative activities that must be retained under the Rules. Accordingly, Cohasset has chosen to use the term "record object" (versus "data," "file" or "object") to consistently recognize that the content is a required record.

1.1.2 FINRA Rule 4511(c) Requirements

Financial Industry Regulatory Authority (FINRA) Rule 4511(c) states: *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.*

1.1.3 CFTC Rule 1.31 Requirements

Effective August 28, 2017, 17 CFR § 1.31 (the "CFTC Rule"), the CFTC defines principles-based requirements for organizations electing to retain electronic regulatory records. These amendments modernize and establish technology-neutral requirements for the form and manner in which regulatory records must be retained and produced.

The definition of *regulatory records* s in 17 CFR § 1.31(a) is essential to the CFTC's electronic recordkeeping requirements.

> *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]

Paragraphs (i) and (ii) include information about how and when such record objects were created, formatted or modified. Similarly, the SEC Rule requires information in addition to the record content by establishing requirements for index data in paragraphs 17a-4(f)(2)(ii)(D), (f)(3)(iv) and (f)(3)(vi) and audit trail data in paragraphs 17a-4(f)(3)(v).

Refer to Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*, which relates the CFTC principles-based requirements to the capabilities of the IBM COS, as described in Section 2. Additionally, refer to Section 5.2, *Overview of CFTC Rule 1.31(c)-(d) Electronic Storage Requirements*.

1.2 Purpose and Approach

To obtain an independent and objective assessment of the compliance capabilities of the IBM COS vault with retention enabled in comparison to the relevant storage-specific requirements set forth in SEC Rule 17a-4(f) and CFTC Rule 1.31(c)-(d), IBM engaged Cohasset Associates, Inc. ("Cohasset"). As a highly-respected consulting firm, Cohasset has recognized expertise and more than 40 years of experience with the legal, technical and operational issues associated with the records management practices of companies regulated by the SEC and the CFTC. Additional information about Cohasset is provided in the last section of this report.

Cohasset was engaged to:

- Assess the capabilities of the IBM COS vault with retention enabled Release 3.12.0, in comparison to the five relevant requirements of SEC Rule 17a-4(f) for recording, storage and retention of electronic record objects and system metadata (system index attributes); see Section 2, Assessment of Compliance with SEC Rule 17a-4(f);
- Associate the principles-based requirements of CFTC Rule 1.31(c)-(d) to the assessed capabilities of the IBM COS vault, with retention enabled; see Section 3, Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d); and
- Prepare this Assessment Report, enumerating the results of its assessment.

In addition to applying the information in this Assessment Report, regulated entities must ensure that the combination of its policies, procedures and regulatory submissions, in conjunction with the capabilities of implemented electronic recordkeeping solutions, meet all applicable requirements of SEC Rule 17a-4(f) and CFTC Rule 1.31.

This assessment represents the professional opinion of Cohasset and should not be construed as either an endorsement, or a rejection, by Cohasset of IBM COS and its capabilities or other IBM products or services. The information utilized by Cohasset to conduct this assessment consisted of: (a) oral discussions, (b) user and system administration documentation, and (c) other directly-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 Cloud Object Storage Overview

The IBM Cloud Object Storage ("COS") is a multipurpose, distributed, object-based storage system designed to store and access unstructured documents. The IBM COS system is a private cloud based architecture that can be deployed (1) on-premise, (2) off-premise (dedicated: single-tenant, or public: multi-tenant, non-IBM public cloud) or (3) as a hybrid mix of on-premise and off-premise. The IBM COS vault with retention enabled is **not** currently available for IBM COS public service from IBM.

IBM COS stores objects in vaults. With an IBM COS vault with retention enabled, retention policies are applied to the vault, or to individual objects, as they are stored. Once a vault with retention enabled is configured, the retention period of the policy applied to individual record objects cannot be shortened, although the policy may be increased or decreased for future stored record objects. Further, legal holds may be applied to record objects, to assure that they are kept longer than the retention period, for special circumstances, such as subpoena, litigation or external investigation. Accordingly, with the IBM COS vault with retention enabled, each record object in the vault is retained as an immutable and undeletable object for at least the duration of the retention policy.

The features of an IBM COS vault with retention enabled are designed to provide stringent retention protection and object management controls with the objective of meeting more rigorous regulatory requirements, such as those in SEC Rule 17a-4(f) and FINRA Rule 4511(c).

2 | Assessment of Compliance with SEC Rule 17a-4(f)

This section presents Cohasset's assessment of the capabilities of the IBM COS vault with retention enabled, for compliance with the five (5) requirements related to recording, storage and retention of electronic records, as stipulated in SEC Rule 17a-4(f).

For each of the five relevant requirements in SEC Rule 17a-4(f), this assessment is organized into the following four topics:

- ***Compliance Requirement*** – Excerpt of each electronic storage requirement in SEC Rule 17a-4(f) and Cohasset's interpretation of the requirement.
- ***Compliance Assessment*** – Assessment of the relevant capabilities of the IBM COS vault with retention enabled Release 3.12.0.
- ***Capabilities of the IBM COS Vault with Retention Enabled*** – Description of relevant capabilities of the IBM COS vault, with retention enabled.
- ***Additional Considerations*** –Additional considerations related to meeting the specific requirement

The following subsections document Cohasset's assessment of the capabilities of the IBM COS vault with retention enabled Release 3.12.0 relative to each pertinent requirement of SEC Rule 17a-4(f).

2.1 Non-Rewriteable, Non-Erasable Record Format

2.1.1 Compliance Requirement [SEC 17a-4(f)(2)(ii)(A)]

As set forth in Section III (B) of the 2001 Interpretive Release, this requirement *"is designed to ensure that electronic records are capable of being accurately reproduced for later reference by maintaining the records in an unalterable form [for the required retention period]."*

SEC 17a-4(f)(2)(ii)(A): Preserve the records exclusively in a non-rewriteable, non-erasable format.

The following statement in the 2003 Interpretive Release further clarifies that certain implementations of rewriteable and erasable media, such as magnetic disk or magnetic tape, meet the requirements of a non-erasable and non-rewriteable recording environment provided: (a) the storage solution delivers the prescribed functionality and (b) the functionality is delivered via appropriate integrated control codes for the SEC designated retention period associated with the stored records.

> *A broker-dealer would not violate the requirement in paragraph (f)(2)(ii)(A) 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.* [emphasis added]

Further, Section IV of the 2003 Interpretive Release places requirements on the storage system for retaining records beyond the SEC-established retention period when certain circumstances occur, such as a subpoena or legal hold:

> *Moreover, there may be circumstances (such as receipt of a subpoena) where a broker-dealer is required to maintain records beyond the retention periods specified in Rule 17a-4 or other applicable Commission rules. Accordingly, 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.* [emphasis added]

This statement by the SEC clarifies that the storage system must have the capability to retain records beyond the retention period established at the time of initial recording when required for legal matters, external investigations or audits, or other similar circumstances.

2.1.2 Compliance Assessment

It is Cohasset's opinion that the storage media capabilities and operational functionality of an IBM COS vault with retention enabled meet this requirement of the Rule to retain *fixed-time*[3] record objects in non-erasable and non-rewriteable format when: (a) the IBM COS vault with retention enabled is properly configured and utilized to store, retain and manage immutable record objects, (b) an appropriate retention policy is applied to the vault with retention enabled, (c) identifiers for legal holds are appropriately applied to the record objects, and (d) the additional considerations identified in Section 2.1.4 are satisfied.

2.1.3 Capabilities of the IBM COS Vault with Retention Enabled

The IBM COS vault with retention enabled capabilities that are directly related to preserving broker-dealer record objects on non-rewritable and non-erasable media, for the required retention period, are presented in this subsection.

System Overview and Components

- IBM COS is a dispersed storage solution for storing and accessing unstructured objects that uses a cluster of storage nodes to store record objects across the available nodes.
- The IBM COS architecture is comprised of the following three functional components (running ClevOS software):
  1. *IBM Cloud Object Storage Manager* provides a management interface that is used for administrative tasks such as system configuration, storage provisioning, and health and performance monitoring of the system.
  2. *IBM Cloud Object Storage Accesser* imports and reads record objects, encrypting/encoding record objects on import and decrypting/decoding record objects on read. It is a stateless component that presents the storage interfaces to the client applications and transforms records objects by using the Information Dispersal Algorithm (IDA).
     - Additionally, *Accesser* utilizes the *Secureslice* feature, by default, which combines all-or-nothing-transform (AONT) encryption with IDA to form a computational secret sharing scheme, thus providing an additional layer of security. AONT is applied as a preprocessing step to IDA.

[3] Fixed-time or time-based retention periods require records to be retained for a specified contiguous period of time from the date and time the record object is created and stored.

3. *IBM Cloud Object Storage Slicestor* is primarily responsible for storage of the record objects slices. It receives record objects from the *Accesser* on import and returns record objects to the *Accesser* as required by the reads. *Slicestor* devices are grouped in *device sets*. Each vault applies the IDA using a *width*[4] and a *threshold*[5] *parameter associated with that vault to transform record object data into the width number of slices such that the original data can be read using a smaller number of slices equal to the threshold*. Slices of a record object are stored across the Slicestor devices in a set such that each Slicestor holds an equal number of slices and no hard drive holds more than one slice associated with that record object.

- IBM COS manages record objects in *vaults, which* are logical containers for storing record objects in a *storage pool*[6]. Vaults can be configured in one of the following two ways:

  1. *Standard* – protection mode is "disabled," or
  2. *Retention* – protection mode is "enabled," indexing is set to "on," and versioning is set to "off." Only empty vaults may be enabled with retention.

Record Object Definition and Controls

- Each record object stored in an IBM COS vault with retention enabled is comprised of two components:

  1. Complete object content. All properly configured record objects received from the regulated entity will be stored, regardless of the content, and are inclusive of all transmitted content.
  2. Object metadata, including both:

     - Immutable (unchangeable) object metadata, such as object name, creation (storage) date and time, retention period, object checksums (MD5 Hash), and user-specified metadata tags for record objects (which are a custom collection of name-value pairs that describe various object qualities).
     - Changeable (mutable) object metadata, including the legal hold identifier, and access control lists (ACL's).

- All attempts to delete a record objects (by users or source applications) prior to the expiration of the retention period and the removal of all associated legal holds, are rejected and tracked as an entry in the audit log.
- The record object name must be unique for the vault where it is stored. If it is not unique, the record object is not stored and an error message is reported through the Cloud Storage Object (CSO) application programming interface (API), which is S3 Compatible.
- A record object may be *copied* between vaults.

  - The storage date and time is the creation date and time for the copy in the destination vault.
  - The retention period applied to the record object must be valid, according to the retention policy of the destination vault, and may be copied from the original record object or set during the copy process.

---

[4] Number of *Slicestor* devices that the data is striped across in a device set and storage pool.

[5] Number of devices that need to be available for the record objects to be readable.

[6] Storage Pools are one or more device sets spread across one or multiple data centers and regions and consists of one or more *device sets*.

- A record object cannot be *moved* between vaults. If this were allowed, the retention period applied to the record object could be shortened, if the new vault had a shorter retention period applied to it.

Retention Policy

The COS vault with retention enabled **must** be configured, via Cloud Storage Object (CSO) API (S3 Compatible) or an administrator through the Manager UI, for each vault.

- *Default retention period*: If the source application does not send a specific retention period, when using PUT, then the vault *default retention period* is stored as the retention period for the record object. Additionally, the *default retention period* is stored when record objects are sent using HTTP POST, even if a specified retention period was provided.
- *Minimum and Maximum retention period*: The minimum and maximum parameters assure that the retention period applied to a record object is equal to or greater than the *minimum* **and** equal to or less than the *maximum* (at the time of initial recording).
  - When a retention period is received that is less than the minimum or greater than the maximum, the PUT object *fails* (meaning that the record object is not stored) and an error message is returned.
  - The Maximum retention period cannot be greater than 70 years.
- The Default, Minimum and Maximum retention periods, can be administratively changed at any time after initial configuration. However, these changes are **not** applied to previously stored record objects.
- Retention periods specified in days are converted internally to milliseconds and stored in the record object metadata.
- The COS vault with retention enabled enforces the retention period and protects the record objects from modification or deletion until the retention period has expired.
- When a delete request is received for an individual record object, the record object's retention period is added to the creation (storage) date/time to determine if the retention period has expired.
- Neither the record object, nor its immutable metadata, can be changed as long as the retention period is in effect. Updates to certain mutable metadata attributes are allowed (such as record access (read) date and time, access permissions, and file owner). These updates do not affect the retention period or controls.
- To aid the system administrator, when object metadata is retrieved (via CSO API GET), the response includes: (a) retention period (in seconds), (b) the calculated retention expiration date, (c) retention legal hold count (number of legal hold identifiers), and (d) content-length.

Fixed Time Retention

Fixed time retention periods define a contiguous duration of time that the record object must be retained, which begins to accrue at the time of the record object was created (stored).

- To be compliant with the Rule, all vaults that store SEC regulated records must be configured as vaults with retention enabled.

- A retention policy must be designated for a vault to enable retention, which assures that a retention period is applied to all record objects. (See *Retention Policy* subsection above for additional information.)
- Legal holds may be applied to individual record objects in vaults with retention enabled.

- A fixed time retention period can be applied and stored as metadata for a record object, using one of two processes:
  1. The vault default retention period is stored as record object metadata, if the source application does not transmit a retention period or a retention expiration date.
  2. A *specified* retention period or retention expiration date may be transmitted with the record object when it is created (stored). The retention expiration date is converted to a retention period (duration of time) and the retention period is stored as record object metadata.
- The retention period stored as record object metadata is added to the creation date and time to calculate the retention expiration date for the record object. The record object content, together with its immutable object metadata, are protected from being deleted, overwritten, or otherwise modified until the calculated retention expiration date has passed.
- The retention period for a stored record object cannot be changed. If a record object needs to be kept for a longer period of time, the Legal Hold feature must be used. (See *Legal Holds* subsection, below, for more information.
- If the default retention period applied to a vault with retention enabled is changed, it only applies to new record objects that are written to the vault. The record objects already stored remain unchanged.

Legal Holds

When a record object is subject to preservation requirements for subpoena, litigation, regulatory investigation or other special circumstances, it must be retained (preserved) as immutable and deletion and overwrites must be prohibited until the hold is removed.

- The Legal Hold feature is enabled when the vault is retention enabled.
- A legal hold identifier is specified by the client and can be up to 64 characters.
- Legal holds are applied via CSO API POST. For each applied legal hold, the identifier and the timestamp when applied are stored for each record object.
  - Up to 100 legal holds may be applied to an individual record object.
  - When one or more legal hold identifiers are applied to the record object, immutability is enforced and both overwrite and deletion of the record object is prohibited, even if the retention expiration date has passed.
  - When all legal hold identifiers are removed, preservation of the record object is no longer mandated by the legal hold identifier(s); however, *other controls* may continue to protect the record object from being changed, deleted, overwritten, archived, or otherwise modified.
- A list of the legal hold identifiers applied to a record object is displayed via the *GET Object Legal Hold* operation.

Deletion

While deletion is **not** required for compliance with the Rule, users may initiate deletion of *eligible* record objects through the CSO API. The record object content, together with its metadata, are *eligible* for deletion when **both of** the following conditions are met:

- Retention expiration date (calculated by adding the record object retention period to the creation (storage) date and time) has passed, and
- No legal hold identifiers are applied to the record object.

Deletion of non-empty vaults is restricted for vaults with retention enabled. Therefore, all record objects in the vault must have been eligible for deletion and deleted before the vault can be deleted. Thus, deleting a vault to effectuate the premature deletion of record objects is prohibited.

Clock Management

The IBM COS vault with retention enabled synchronizes time with a network protocol clock (NTP) to ensure that the local clock is set correctly. A periodic check is made against the NTP clock to keep the local clock within a 1000 second threshold.

- If the clock is off by less than 1000 seconds the NTP daemon begins adjusting the local clock towards the remote clock time, using drifting (slow, very small adjustments of approximately 1-2 seconds per hour) until the clocks are in sync.
- If the clock is off by more than 1000 seconds, the server is taken off-line and is immediately adjusted to match the remote clock and an entry is created in the audit log.

This process ensures that timestamps are accurately recorded when the record object and metadata are written. In addition, it ensures that the clock cannot be temporarily advanced to enable the ability to prematurely delete record objects.

Security

In addition to the stringent retention protection and management controls described above, IBM COS provides the following security capabilities, which support the authenticity and reliability of the record objects.

- Role-Based Access Control – security is set-up and managed in the Manager UI and provides the means to create, delete, and maintain accounts via the *Security* tab. The *Security* tab access can be restricted to a Security Officer, which provides the ability to independently assign and control user permissions.
  - Records of actions taken are kept on the Manager Web Interface.
  - Separate accounts for each administrator can be created to allow only specific system administrators the ability to perform a specific task.
    - Users are only able to perform tasks that are associated with the roles that are assigned to their account.
- Limit vault access by IP – provides protection from unauthorized mounts and access through an IP filtering access control list and assigned vault users.

- *SecureSlice,* – combines all-or-nothing-transform (AONT) encryption with IDA to form a computational secret sharing scheme to further protect the record objects.
  - SecureSlice does not require a key management system.
  - RC4-128 Encryption with MD5-128 hash is the default configuration, although AES-256 Encryption with SHA-256 hash may be enabled.
- Secure Communication – communication with the Cloud Object Storage Manager is always encrypted by using HTTPS, SSL tunneling, and SNMPv3 data protection.
- Transport Layer Security (TLS) with AES – Ensures that all network traffic between appliances in IBM COS is encrypted.
- AWS V4 Authentication – Is required for all Write/Delete operations of vaults with retention enabled and requires adding authentication information (an access key) to the requests.
  - Anonymous access is not supported for vaults with retention enabled.

2.1.4 Additional Considerations

The following additional considerations for configuring and using an IBM COS vault with retention enabled are provided to support compliance with the non-erasure and non-rewritable requirement of the Rule for the full time-period that the record objects are required to be retained. The regulated entity is responsible for:

- Configuring the vault(s) that will be used to store SEC regulated record objects, as vault(s) with retention enabled; thereby establishing the foundation for meeting the requirements of the Rule.
- Configuring the retention policies with minimum, maximum, and default retention periods that meet regulatory requirements when the vault is created with retention enabled.
- Ensuring all complete record objects required to be retained for compliance with the Rule are successfully stored in an IBM COS vault with retention enabled within 24 hours of creation, or are stored in an SEC-compliant protected storage system until they are uploaded to an IBM COS vault with retention enabled.
- Ensuring that an appropriate retention period is applied to the record object, when it is stored, since the retention period cannot be modified once it is written.
- Applying Legal Holds to record objects that: (a) require preservation for legal matters, government investigations, external audits and other similar circumstances, and (b) require retention beyond the originally applied retention period.
- Storing record objects requiring event-based retention periods in a separate compliance system, since the IBM COS does not currently support event-based retention periods.
- Establishing and maintaining appropriate security controls and protocols.
- Configuring and synchronizing the clock with an NTP clock and regularly (about every 60 seconds) comparing the clock to the NTP clock and resynchronized, as required.

2.2 Accurate Recording Process

2.2.1 Compliance Requirement [SEC 17a-4(f)(2)(ii)(B)]

The intent of this requirement is to ensure both the accuracy and quality of the recording process such that the records read from the storage media are precisely the same as those that were recorded. This requirement includes both a quality verification of the recording process and post-recording verification processes.

SEC 17a-4(f)(2)(ii)(B): Verify automatically the quality and accuracy of the storage media recording process.

2.2.2 Compliance Assessment

It is Cohasset's opinion that the use of checksums and validation processes by an IBM COS vault with retention enabled in conjunction with the inherent capabilities of advanced electronic recording technology, meet this requirement of the Rule to verify the accuracy and quality of the recording process.

2.2.3 Capabilities of the IBM COS Vault with Retention Enabled

The recording and the post-recording verification processes of the IBM COS vault with retention enabled are described below.

Recording Process:

- As part of the record object upload process, the regulated entity's source application must provide a checksum (MD5 Hash) of the record content. The record object is only stored if the checksum calculated by the IBM COS vault with retention enabled matches the checksum provided by the source application. If it does not match, the record object is rejected and an error is reported to the regulated entity (via the audit log). The record object must be re-uploaded.
- When a record object is uploaded to the IBM COS vault with retention enabled an 'ok' response is sent to the source application.
- The IBM COS vault with retention enabled stores the checksum in the record object metadata. The checksum is immutable and is used in the post-recording period to verify the integrity of the record object.
- The IBM COS vault with retention enabled utilizes advanced electronic recording technology which applies a combination of checks and balances, such as inter-component and inter-step cyclical redundancy checks (CRCs) and write-error detection and correction, to assure that record objects are written in a high quality and accurate manner.

Post-Recording Verification Process:

- Integrity of the record object is validated by comparing the checksum of each slice of a record object on each read, to ensure that an accurate record object is delivered.
  - If a slice is determined to be corrupt, meaning the integrity check value is invalid, the slice is rejected and rebuilt on the IBM COS vault with retention enabled from the other slices making up the record object.

- The IBM COS vault with retention enabled employs an intelligent background process that periodically scans storage nodes, checking and correcting errors. Integrity of the stored record object slices is validated by the Slicestor appliance., If a slice is determined to be corrupt, meaning the integrity check value is invalid, the distributed rebuilder technology is initiated.
  - Rebuilder Agents are designed to correct error conditions, which may be detected when portions of dispersed record objects are missing from their respective storage nodes or may be corrupt on-disk.
  - Rebuilder Agents operate continually on all Slicestor enabled storage appliances.

2.2.4 Additional Considerations

There are no additional considerations related to this requirement.

2.3 Serialize the Original and Duplicate Units of Storage Media

2.3.1 Compliance Requirement [SEC 17a-4(f)(2)(ii)(C)]

This requirement, according to Section III(B) of the SEC's 2001 Interpretive Release, *"is intended to ensure both the accuracy and accessibility of the records by indicating the order in which records are stored, thereby making specific records easier to locate and authenticating the storage process."*

SEC 17a-4(f)(2)(ii)(C): Serialize the original and, if applicable, duplicate units of storage media, and time-date for the required period of retention the information placed on such electronic storage media.

When the SEC Rule was issued in 1997, this requirement was thought to be more pertinent to tracking the individual units of removable media related to micrographic or optical storage. This requirement for non-unitized electronic storage may be satisfied by capturing and storing immutable metadata, associated with each electronic record, to *uniquely* identify the record and the *date and time of recording*.

2.3.2 Compliance Assessment

Cohasset believes that the capabilities of an IBM COS vault with retention enabled meet this requirement of the Rule for serializing the record objects by storing a unique ObjectID and a creation (storage) date, as immutable metadata for the record object.

2.3.3 Capabilities of the IBM COS Vault with Retention Enabled

- The IBM COS vault with retention enabled uses the record object name as the identifier and does not allow for the creation of duplicate record object names.
- The IBM COS vault with retention enabled assigns an ObjectID, which identifies the record object. The ObjectID is then mapped in a single Global Namespace.
- Further, the creation (storage) date and time is stored with each record object in the vault with retention enabled and is immutable.
- The combination of the unique ObjectID and the creation (storage) date and time provide a serialization of each record object in both space and time.

2.3.4 Additional Considerations

There are no additional considerations related to this requirement.

2.4 Capacity to Download Indexes and Records

2.4.1 Compliance Requirement [SEC 17a-4(f)(2)(ii)(D)]

This requirement necessitates an adequate capacity to readily download records and associated indexes, in a format and on a medium acceptable under the Rule and as specified by the SEC or self-regulatory organization. This allows the SEC or self-regulatory organizations to take possession of the downloaded records and indexes.

SEC 17a-4(f)(2)(ii)(D): Have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable under this paragraph (f) as required by the Commission or the self-regulatory organizations of which the member, broker, or dealer is a member.

2.4.2 Compliance Assessment

It is Cohasset's opinion that an IBM COS vault with retention enabled supports the regulated entity in meeting this requirement by providing LIST and GET tools for authorized users to readily download the record objects and metadata (index) attributes. These record objects and metadata (index) attributes can then be transferred by the regulated entity to a compliant media, as required.

2.4.3 Capabilities of the IBM COS Vault with Retention Enabled

Record objects and metadata (index) attributes may be downloaded using the CSO API. The following capabilities support the capacity to download record objects and metadata (index) attributes:

- The IBM COS vault provides GET and LIST tools to access the record objects and metadata (index) attributes.
- With the CSO API, authorized users can: (a) list record objects and their associated metadata, (b) search the object name, and (c) download the record object and associated metadata (index) attributes to a designated storage location. Record object metadata (index) attributes, include:
  - Immutable object metadata, e.g., object name, creation (storage) date and time, and size.
  - Changeable object metadata includes Legal Hold identifiers and ACL's.

2.4.4 Additional Considerations

The regulated entity is responsible for authorizing user access, maintaining the IBM COS vault settings, and assuring that the SEC, CFTC, self-regulatory organization or designated examining authority receive downloads of the record objects and metadata (index) attributes, in the requested form and medium.

2.5 Duplicate Copy of the Records Stored Separately

2.5.1 Compliance Requirement [SEC 17a-4(f)(3)(iii)]

The intent of this requirement is to provide an alternate storage source for accessing the records, should the primary source be compromised, i.e., lost or damaged.

SEC 17a-4(f)(3)(iii): Store separately from the original, a duplicate copy of the record stored on any medium acceptable under §240.17a-4 for the time required.

Note: A *duplicate copy* allows for the complete and accurate record to be reestablished from data stored on a compliant storage system or media. Whereas, a *backup copy* is defined as a non-persistent copy that is overwritten as it is *rotated* on a periodic basis, resulting in a much shorter retention period than the original.

2.5.2 Compliance Assessment

It is Cohasset's opinion that an IBM COS vault with retention enabled meets this SEC requirement for a duplicate copy through erasure coding, when the vault is configured to store coded slices of the record object across three or more data centers. Should an error be encountered in one or more slices, the stored record object is regenerated from valid erasure coded slices stored on other storage devices.

2.5.3 Capabilities of the IBM COS Vault with Retention Enabled

- Each vault with retention enabled is part of a *storage pool* which contains a width number of *Slicestor* devices in a *device set*. Each record object is transformed into slices by the Information Dispersal Algorithm (IDA). The number of slices is equal to the IDA width of the vault in which the record object data is stored. The width number of slices created from the data are striped across all the Slicestors in a *device set*. This assures that the record object and associated metadata (index) attributes are recoverable by regenerating a duplicate of the original from erasure encoded data.
  - Record objects added to the vault use the preconfigured *IDA width of Slicestor devices*.
  - Once configured, the *width* of the vault cannot be decreased, although in certain circumstances it can be increased which results in increased durability of object data contained in that vault.
  - Storage pools can be spread across multiple data centers, which can be geographically distant from one another.
- The erasure coded data slices are retained for the full retention period of the record object and any applied Legal Holds.

2.5.4 Additional Considerations

Cohasset ***recommends*** the regulated entity configure the system such that the storage pools used for the COS vault with retention enabled are equally distributed across three or more geographically dispersed data centers. A deployment using only one or two data centers is **not** supported.

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

The objective of this section is to document Cohasset's assessment of the capabilities of the IBM Cloud Object Storage Release 3.12.0 in comparison to the CFTC requirements.

The individual relevant requirements cited in Section 2, *Assessment of Compliance with SEC Rule 17a-4(f)*, are based on the wording in SEC Rule 17a-4(f) and Cohasset's interpretation of the requirements, given the associated SEC Interpretive Releases. Specifically, the SEC's 2003 Interpretive Release reiterates that the Rule sets forth standards that the electronic storage media must satisfy to be considered an acceptable method of storage under Rule 17a-4:

> *A broker-dealer would not violate the requirement in paragraph (f)(2)(ii)(A) 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.* [emphasis added]

Accordingly, it is Cohasset's opinion that the requirements set forth in SEC Rule 17a-4(f) are *technology-neutral* and apply to any electronic solution with (a) integrated control codes that extend to the electronic storage system and (b) features that deliver capabilities that meet the requirements of the Rule.

The August 28, 2017, amendments to CFTC Rule 1.31 establish *technology-neutral*, *principle-based* requirements. As illustrated in the table in this section, it is Cohasset's opinion that the requirements of the modernized CFTC Rule may be achieved by meeting the SEC requirements.

When comparing the capabilities of the IBM COS vault with retention enabled that align with the SEC requirements to the *principles-based* CFTC requirements, it is essential to recognize that the SEC Rule separately describes requirements for index data and audit trail, whereas the CFTC in 17 CFR § 1.31(a) establishes an expanded definition of an electronic regulatory record to include the information as specified in paragraph (i) and (ii) below.

> ***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 table below lists the *principles-based* CFTC requirements related to the *form and manner of retention* and the *inspection and production of regulatory records*. The middle column also provides Cohasset's analysis and opinion regarding the ability of the IBM COS vault with retention enabled to meet the requirements for electronic regulatory records in CFTC Rule 1.31(c)-(d). In addition, for ease of reference the SEC requirements described in the sections referenced in the middle column are listed.

CFTC 1.31(c)-(d) Requirement	Compliance Assessment Relative to CFTC 1.31(c)-(d)	SEC 17a-4(f) Requirements Listed in the Referenced Sections
(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 capabilities described in Sections 2.1 through 2.4 meet CFTC requirements (c)(1) and (c)(2)(i) for record objects. Additionally, for *records stored electronically*, the CFTC has expanded the definition of *regulatory records* in 17 CFR § 1.31(a) to include metadata: *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] It is Cohasset's opinion that the IBM COS vault with retention enabled retains the immutable metadata (index attributes) as an integral part of record object; and, therefore are subject to the same retention protections as the associated record object. Immutable record object metadata includes *object name, creation (storage) date and time, retention period and object checksums (MD5 Hash) and user-specified metadata tags (which are a custom collection of name-value pairs that describe various object qualities).* Additionally, mutable (changeable) metadata attributes stored for a record object include *legal hold identifier(s), access control lists (ACLs). The most recent values of mutable metadata are retained for the same time period as the associated record object.* To satisfy this requirement for other essential data related to how and when the record objects were created, formatted, or modified, the regulated entity must retain this data in a compliant manner.	Section 2.1 *Non-Rewriteable, Non-Erasable Record Format* *Preserve the records exclusively in a non-rewriteable, non-erasable format.* [SEC 17a-4(f)(2)(ii)(A)] Section 2.2 *Accurate Recording Process* *Verify automatically the quality and accuracy of the storage media recording process.* [SEC 17a-4(f)(2)(ii)(B)] Section 2.3 Serialize the Original and Duplicate Units of Storage Media *Serialize the original and, if applicable, duplicate units of storage media, and time-date for the required period of retention the information placed on such electronic storage media.* [SEC 17a-4(f)(2)(ii)(C)] *Section 2.4 Capacity to Download Indexes and Records* *Have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable under this paragraph (f) as required by the Commission or the self-regulatory organizations of which the member, broker, or dealer is a member.* [SEC 17a-4(f)(2)(ii)(D)]
(ii) Systems that ensure the records entity is able to produce electronic regulatory records[7] 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 the capabilities of the IBM COS vault with retention enabled as described in Section 2.5, *Duplicate Copy of the Records Stored Separately*, 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*. Specifically, section 2.5 explains that durability is achieved through erasure coding when the IBM COS vault with	*Section 2.5 Duplicate Copy of the Records Stored Separately* *Store separately from the original, a duplicate copy of the record stored on any medium acceptable under §240.17a-4 for the time required.* [SEC 17a-4(f)(3)(iii)]

[7] 17 CFR § 1.31(a) includes indices (*Any data necessary to access, search, or display any such books and records*) in the definition of regulatory records.

CFTC 1.31(c)-(d) Requirement	Compliance Assessment Relative to CFTC 1.31(c)-(d)	SEC 17a-4(f) Requirements Listed in the Referenced Sections
	retention enabled is configured to store coded slices of the record object and associated immutable and mutable metadata across three or more data centers. To satisfy this requirement for other essential data related to how and when the record objects were created, formatted, or modified, the regulated entity must retain this data in a compliant manner.	
(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).	N/A
(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 the IBM COS vault with retention enabled has features that support the regulated entity's efforts to comply with requests for inspection or production of record objects and associated system metadata (i.e., index attributes). Specifically, it is Cohasset's opinion that Section 2.4, *Capacity to Download Indexes and Records*, describes use of the IBM COS vault to retrieve and download the record objects and the associated metadata retained by the IBM COS vault with retention enabled. Further, as noted in the *Additional Considerations* in Section 2.4.4, the regulated entity is obligated to produce the record objects and associated metadata, in the form and medium requested. If the regulator requests additional data related to how and when the record objects were created, formatted, or modified, the regulated entity will need to provide this information from appropriate source systems.	*Section 2.4 Capacity to Download Indexes and Records* *Have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable under this paragraph (f) as required by the Commission or the self-regulatory organizations of which the member, broker, or dealer is a member.* [SEC 17a-4(f)(2)(ii)(D)]

4 | Conclusions

Cohasset assessed the capabilities of the IBM Cloud Object Storage (COS) vault with retention enabled, Release 3.12.0, in comparison to the five requirements related to recording, storage and retention of record objects and associated metadata, set forth in SEC Rule 17a-4(f) and its associated Interpretive Releases. Cohasset also correlated the principles-based requirements in CFTC Rule 1.31(c)-(d) to the assessed capabilities of the IBM Cloud Object Storage vault with retention enabled.

Cohasset determined that the IBM COS vault with retention enabled has the following capabilities, which support its ability to meet the recording, storage and retention requirements:

- Maintains record objects and immutable record object metadata in a non-erasable and non-rewriteable format for fixed-time retention periods.
- Allows legal holds to be applied to record objects subject to preservation requirements, which retains (preserves) the record object as immutable and prohibits deletion or overwrites until the Legal Hold identifiers are removed.
- Prohibits deletion of a record object and its immutable metadata until the associated retention period has expired.
- Encrypts record object, by default, using RCA-128 Encryption.
- Verifies the accuracy and quality of the recording process automatically utilizing (a) advanced storage recording technology, and (b) a checksum (MD5 Hash). that is received from the host system during the recording process and is stored as a metadata attribute and utilized for post-recording verification.
- Uniquely identifies and chronologically serializes each stored record object.
- Allows authorized users to access the record objects and metadata with CSO API for local reproduction or transfer to a format and medium acceptable under the Rule.
- Regenerates an accurate replica of the record object and metadata (including index attributes) from valid erasure coded slices, should one of the recorded slices become lost or damaged.

Accordingly, Cohasset concludes that the IBM COS vault with retention enabled when properly configured and utilized to store and retain time-based records, meets the requirements that relate directly to the recording, storage and retention of record objects and system metadata.

5 | Overview of Relevant Regulatory 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 allowing electronic records to be retained on a variety of compliant electronic storage media.

5.1 Overview of SEC Rule 17a-4(f) Electronic Records Storage Requirements

Recordkeeping requirements for the securities broker-dealer industry are stipulated by the United States Securities and Exchange Commission ("SEC") Regulations, including 17 CFR §§ 240.17a-3 and 240.17a-4. Specifically, SEC Rule 17a-4(f), when adopted on February 12, 1997, expressly allow books and records to be retained on electronic storage media, subject to meeting certain conditions.

Three separate foundational documents collectively define and interpret the specific regulatory requirements that must be met for an electronic storage system to be compliant with SEC Rule 17a-4(f). These are:

- The Rule itself, as modified over time by the SEC. These modifications to the original Rule have not affected the requirements for electronic storage media, which are the basis of this assessment. However, certain Interpretive Releases have clarified the context and meaning of certain requirements and conditions of the Rule.
- SEC Interpretive Release No. 34-44238, *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)*, dated May 1, 2001 (the "2001 Interpretive Release").
- SEC Interpretive Release No. 34-47806, *Electronic Storage of Broker-Dealer Records*, dated May 7, 2003 (the "2003 Interpretive Release").

In the Rule and in the two subsequent interpretative releases, the SEC authorizes the use of electronic storage media and devices to satisfy the recordkeeping requirements of Rules 17a-3 and 17a-4, when the system delivers the prescribed functionality. Specifically, Rule 17a-4(f)(1)(ii) states:

> *(f) The records required to be maintained and preserved pursuant to §§ 240.17a-3 and 240.17a-4 may be immediately produced or reproduced on "micrographic media" (as defined in this section) or by means of "electronic storage media" (as defined in this section) that meet the conditions set forth in this paragraph and be maintained and preserved for the required time in that form.*
> *(1) For purposes of this section:*
> *(ii) The term electronic storage media means any digital storage medium or system and, in the case of both paragraphs (f)(1)(i) and (f)(1)(ii) of this section, that meets the applicable conditions set forth in this paragraph (f). [emphasis added]*

The February 12, 1997, Federal Register issued the final rule allowing broker-dealers to use electronic storage media. When issuing the rule, the SEC recognized that technology evolves and it set forth standards that the electronic storage media must satisfy, rather than prescribing specific technology, as specified in the following excerpts:

> ***SUMMARY:*** *The Securities and Exchange Commission ("Commission") is amending its broker-dealer record preservation rule to allow broker-dealers to employ, under certain conditions, electronic storage media to maintain records required*

> *to be retained. The amendments reflect a recognition of technological developments that will provide economic as well as time-saving advantages for broker-dealers by expanding the scope of recordkeeping options while at the same time continuing to require broker-dealers to maintain records in a manner that preserves their integrity. The Commission is also issuing an interpretation of its record preservation rule relating to the treatment of electronically generated communications.*
> ***
> ***II. Description of Rule Amendments***
> ***A. Scope of Permissible Electronic***
> ***Storage Media***
> ****The Commission is adopting a rule today which, instead of specifying the type of storage technology that may be used, sets forth standards that the electronic storage media must satisfy to be considered an acceptable method of storage under Rule 17a–4. Specifically, because optical tape, CD–ROM, and certain other methods of electronic storage are available in WORM and can provide the same safeguards against data manipulation and erasure that optical disk provides, the final rule clarifies that broker-dealers may employ any electronic storage media that meets the conditions set forth in the final rule.*[8] [emphasis added]

The 2003 Interpretive Release further clarifies that implementation of rewriteable and erasable media, such as magnetic tape or magnetic disk, meets the requirements of a non-erasable and non-rewriteable recording environment, if the system delivers the prescribed functionality and appropriate **integrated control codes** are in place. The 2003 Interpretive Release states:

> *A broker-dealer would not violate the requirement in paragraph (f)(2)(ii)(A) 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.* [emphasis added]

The key words within this statement are "integrated" and "control codes." The term "integrated" means that the method used to achieve a non-rewriteable, non-erasable recording environment must be an integral part of the recording hardware and software. The term "control codes" indicates the acceptability of using attribute codes (metadata), which are integral to the hardware and software of the recording process, to protect against overwriting or erasure of any records.

Examples of integrated control codes relevant to a non-rewriteable and non-erasable recording process are:

- A retention period during which the record object cannot be erased, overwritten or otherwise modified;
- A unique record identifier that differentiates each record from all other records; and
- The date and time of recording, which in combination with the unique identifier "serializes" the record.

The 2003 Interpretive Release specifically notes that recording processes or applications which merely mitigate the risk of overwrite or erasure (rather than prevent them), such as relying solely on access control security, will not satisfy the requirements of SEC Rule 17a-4(f).

Further, the 2003 Interpretive Release requires the storage system to be capable of retaining records beyond the SEC-established retention period, when required by a subpoena, legal hold or other similar circumstances. In *Section IV. Discussion*, the 2003 Interpretive Release states:

[8] Exchange Act Release No. 38245 (Feb. 5, 1997), 62 FR 6469 (Feb. 12, 1997) ("Adopting Release").

> *Moreover, there may be circumstances (such as receipt of a subpoena) where a broker-dealer is required to maintain records beyond the retention periods specified in Rule 17a-4 or other applicable Commission rules. Accordingly, 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. [emphasis added]*

An important associated requirement of SEC Rule 17a-4(f)(2)(i) is that a member, broker or dealer electing to electronically store its records required by SEC Rules 17a-3 or 17a-4, must notify its designated examining authority at least ninety (90) days prior to employing any technology other than write-once read-many ("WORM") optical media. Examining authorities are self-regulatory organizations (SROs) or designated examining authorities (DEAs) under the jurisdiction of the SEC, such as the Financial Industry Regulatory Authority (FINRA).

See Section 2, Assessment of Compliance with SEC Rule 17a-4(f), for a list of the *five* SEC requirements relevant to the recording, storage and retention of electronic records and a description of the capabilities of IBM Cloud Object Storage related to each requirement.

5.2 Overview of FINRA Rule 4511(c) Electronic Records Storage Requirements

Financial Industry Regulatory Authority (FINRA) Rule 4511(c) explicitly defers to SEC Rule 17a-4(f), by stipulating:

> *(c) 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 Rule 17a-4.*

5.3 Overview of CFTC Rule 1.31 Electronic Regulatory Records Requirements

Effective August 28, 2017, the Commodity Futures Trading Commission (CFTC) amended 17 CFR § 1.31 ("CFTC Rule") to define principles-based requirements for organizations electing to retain electronic regulatory records. The CFTC requirements for electronic regulatory records evolved through amendments to Rule 1.31. The most substantive changes included:

- The June 28, 1999, amendment first implemented the technical provisions regarding the use of electronic storage media for required books and records.
- The November 2, 2012, amendment clarified the retention period for certain oral communications.
- The August 28, 2017, amendments modernize and make technology-neutral the form and manner in which regulatory records, including electronic regulatory records, must be retained and produced.

To address the transition to electronic regulatory records, the CFTC amended and modernized its recordkeeping regulation to adopt principles-based standards that are less prescriptive. This resulted in rephrasing and modernizing the requirements previously defined in 1999, as explained in the August 28, 2017, Federal Register in *III. Final Rules, D. Regulation 1.31(c): Form and Manner of Retention:*

> *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. The Commission proposed to adopt § 1.31(d)(2) to set forth additional controls for records entities retaining electronic regulatory records. The Commission emphasized in the Proposal that the proposed regulatory text does not create new requirements, but*

> *rather updates the existing requirements so that they are set out in a way that appropriately reflects technological advancements and changes to recordkeeping methods since the prior amendments of § 1.31 in 1999.* [emphasis added]

The definitions established in 17 CFR § 1.31(a) are paramount to applying the CFTC requirements.

> *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]

These definitions establish that recordkeeping obligations apply to (a) all *records entities*, without exception, and (b) 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 record objects, as well as information describing how and when such books and records were created, formatted, or modified.

The retention time periods for regulated records includes both time-based[9] and event-time-based[10] retention periods. Specifically, 17 CFR § 1.31 (b)(1)-(b)(3) 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.* [emphasis added]

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

[9] Time-based retention periods require the record object to be retained for a specified contiguous period of time from the date and time the record object is created and stored.

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

About Cohasset Associates, Inc.

Cohasset Associates, Inc. (www.cohasset.com) is recognized as a leading professional consulting firm, specializing in records management and information governance. Drawing on more than forty 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, engaging in implementation activities to promote interdisciplinary information governance, achieve business objectives, optimize information value, improve compliance, and mitigate information-related risk.

Cohasset has been 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.

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 assists with the implementation of information lifecycle practices that avoid the cost and risk associated with over-retention*
- *Defines technical and functional requirements and assists with the deployment of enterprise content management and collaboration tools*

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

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