Cohasset Associates

SEC 17a-4(f), FINRA 4511(c) & CFTC 1.31(c)-(d) Compliance Assessment
Alibaba Cloud Object Storage Service

Abstract

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.

Object Storage Service (OSS) on the global Alibaba Cloud Platform offers highly scalable storage and archiving capabilities for objects including unstructured data, documents, images, audio and video files. The *OSS Retention Strategy* feature is designed to meet securities industry requirements for preserving records in a non-rewriteable and non-erasable format. An *OSS Retention Strategy*, when properly configured and *locked*, applies integrated control codes to prevent stored records from being modified, overwritten, or deleted, until the specified retention period has expired and any associated legal holds have been released.

In this Assessment Report, Cohasset Associates, Inc. (Cohasset) assesses the functionality of the Alibaba Object Storage Service, with a locked *OSS Retention Strategy,* relative to the recording, storage, and retention requirements specified in:

- 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), which defers to the format and media requirements of SEC Rule 17a-4(f).

- Commodity Futures Trading Commission (CFTC) in regulation 17 CFR § 1.31(c)-(d), which regulates commodity futures trading.

It is Cohasset's opinion that Alibaba Cloud Object Storage Service, when used with locked *OSS Retention Strategies*, retains time-based records in a non-erasable and non-rewriteable format and meets the five relevant storage requirements of SEC Rule 17a-4(f), FINRA Rule 4511(c), and the principles-based requirements of CFTC Rule 1.31(c)-(d).

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

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[2] on electronic storage media. Additionally, effective August 28, 2017, the Commodity Futures Trading Commission (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 Alibaba OSS Retention Strategy feature was designed to meet the stringent electronic records requirements for the recording, storage and retention of regulated books and records. To evaluate its compliance with the SEC and CFTC requirements, Alibaba engaged Cohasset to complete an independent and objective assessment of the capabilities of the Object Storage Service with the OSS Retention Strategy feature, 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 the Alibaba Object Storage Service.*

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 "Rule 17a-4"). These amendments to paragraph (f) expressly allow books and records 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, <u>sets forth standards that the electronic storage media must satisfy</u> 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).

Refer to Section 5.1, Overview of SEC Rule 17a-4(f) Electronic Records Storage Requirements, for a summary of the SEC Rule and these two Interpretive Releases.

---

[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 used the term *record object* (versus *data* or *object*) to consistently recognize that the data or object is a required record.

1.1.2   FINRA Rule 4511(c) Requirements

Financial Industry Regulatory Authority (FINRA) Rule 4511(c) explicitly defers to the format and media requirements of SEC Rule 17a-4, for the 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.*

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* 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 [Product Name], as described in Section 2. Additionally, refer to Section 5.3, *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 Alibaba Cloud Object Storage Service, with the OSS Retention Strategy feature, in comparison to relevant storage-specific requirements set forth in SEC Rule 17a-4(f) and CFTC Rule 1.31(c)-(d), Alibaba 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 Object Storage Service with the *OSS Retention Strategy* feature, in comparison to the five requirements of SEC Rule 17a-4(f) for recording, storage and retention of electronic record objects and associated metadata; 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 Object Storage Service with the *OSS Retention Strategy* feature; 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 Object Storage Service and its capabilities or other Alibaba products or services. The information utilized by Cohasset to conduct this assessment consisted of: (a) oral discussions, (b) system documentation, (c) user and system administrator guides, and (d) other directly-related materials provided by Alibaba 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 Alibaba Object Storage Service Overview

Alibaba Cloud is a secure cloud services platform that provides compute, storage, database, content delivery and other functionality to help businesses scale and grow globally. Object Storage Service (OSS) is an Alibaba Cloud service that provides highly scalable and secure storage and archiving capabilities for objects such as unstructured data, documents, images, audio and video files. Three different classes of storage are available, based on performance and cost requirements. The stored objects can be accessed securely from anywhere in the world.

An Alibaba Cloud Account (i.e., Alibaba customer) stores record objects in containers called Buckets, within one or more designated OSS Regions. The *OSS Retention Strategy* feature was designed to store record objects in compliance with SEC Rule 17a-4(f) and other similar regulatory requirements. When an *OSS Retention Strategy* with a retention period is defined and *locked* for a Bucket, integrated controls are applied which prevent the modification, overwrite or premature deletion of the Bucket's record objects for the designated retention period. Additionally, a legal hold may be applied to a Bucket to immutably preserve all record objects stored in the Bucket for purposes of subpoena, litigation, regulatory investigation, and other similar circumstances, for the duration of the hold.

This assessment focuses on the Alibaba Cloud Object Storage Service and the specific features that are relevant for meeting the five storage requirements of SEC Rule 17a-4(f), FINRA Rule 4511(c), and the principles-based requirements of CFTC Rule 1.31(c)-(d).

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

This section presents Cohasset's assessment of the capabilities of Alibaba Object Storage Service, with the OSS Retention Strategy feature, 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 Alibaba Cloud Object Storage Service with the *OSS Retention Strategy* feature

- **Alibaba Cloud Object Storage Service Capabilities** – Description of relevant capabilities of the assessed service

- **Additional Considerations** – Additional considerations related to meeting the specific requirement

The following subsections document Cohasset's assessment of the capabilities of the Alibaba Cloud Object Storage Service, with the *OSS Retention Strategy* feature, 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 <u>prevents the overwriting, erasing or otherwise altering of a record during its required retention period</u> through the use of <u>integrated</u> hardware and software <u>control codes</u>.* [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 <u>the broker-dealer's storage system must allow records to be retained beyond the retentions periods specified in Commission rules</u>. [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 Alibaba Cloud Object Storage Service, when utilized with the *OSS Retention Strategy* feature, meets this SEC requirement to retain records in a non-erasable and non-rewriteable format, when (a) utilized to retain record objects that require time-based[3] retention, (b) an appropriate retention period is assigned to the *OSS Retention Strategy*, (c) the *OSS Retention Strategy* is locked, (d) legal holds are appropriately set to preserve all record objects in the Bucket for purposes of litigation and other similar circumstances, and (e) the considerations identified in Section 2.1.4 are satisfied.

2.1.3   Alibaba Cloud Object Storage Service Capabilities

Overview

▶ The Object Storage Service (OSS) provides the ability to store unlimited amounts of data, such as documents, images, audio or video objects in the cloud, within one or more designated OSS Regions.

▶ Three classes of storage are available within each OSS Region to store data according to its lifecycle status (hot data to cold data):

- <u>Standard</u> – highly available, high-performance storage used for data and objects requiring frequent access.

- <u>Infrequent Access</u> – lower cost storage for data and objects requiring less frequent real-time access, such as longer-term backups.

- <u>Archive</u> – lowest cost, highest latency storage that is best suited to long-term archival of cold objects.

▶ Figure 1 illustrates the storage hierarchy utilized within OSS.

- An Enterprise Account may deploy the Object Storage Service in one or more geographic Regions, based on cost and performance requirements.

    ◆ Each Region is composed of one or more *Availability Zones,* i.e., clusters of one or more independent data centers, designed to offer high availability and error tolerance capabilities.
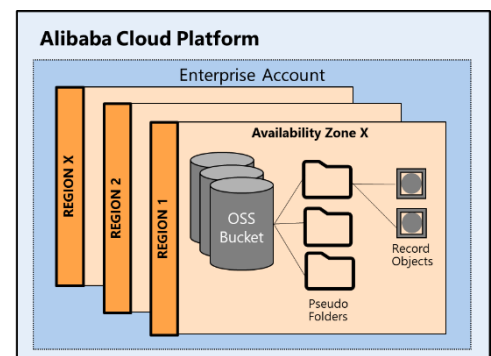

Figure 1: Storage Hierarchy

---

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

- Record objects are stored in containers, called Buckets.

  - A maximum of 30 Buckets are allowed per Region.

  - A Bucket, once created, cannot be moved to another Region, however, it may be copied.

- Record objects are uploaded to a Bucket via the OSS User Console, OSS Software Development Kits (SDKs) or RESTful Application Programming Interfaces (APIs). Both single and multi-part uploads are allowed.

- Within each Bucket:

  - Record objects are stored in a flat file structure, however, pseudo file folders (i.e. classification tags prefixed to the file name) can be used to emulate a hierarchical, directory-based file system. There is no limit to the number of record objects or folders that may be contained within a Bucket.

  - Record objects are assigned a tag which indicates their individual storage class (i.e. Standard, Infrequent Access, and Archive). Multiple storage classes are allowed within a single Bucket.

  - Record objects stored in the Object Storage Service cannot be modified directly. However, record objects may be appended to, or overwritten by a new record object with the same name. *Note: replacing, or appending to, a record object is prohibited when it is stored in a Bucket with a locked OSS Retention Strategy (see below).*

▶ Retention is applied at the Bucket level, via an *OSS Retention Strategy*, with an appropriate retention period that applies to all contents of the Bucket. (See *Record Object and Retention Controls* section for more detail.) Once an *OSS Retention Strategy* is applied to a Bucket <u>and locked</u>, integrated control codes are applied to ensure that:

- Record objects are protected against modification or overwrite for the specified retention period.

- Record objects cannot be deleted through any mechanism until the assigned retention period expires and any Bucket-level Legal Holds are lifted.

- The *OSS Retention Strategy* for the Bucket cannot be deleted.

- The retention period (duration of time) cannot be shortened for the Bucket, only extended.

Record Object and Retention Controls

▶ The term "record object" is used to designate all elements of a file that is uploaded to and stored in an OSS Bucket. A record object is comprised of the following elements:

- Content, such as unstructured data, images, audio or video content.

- Key, which is the record object's unique name within the bucket, as provided by the customer.

- Metadata:

  - *Immutable* – critical attributes of the record object such as the last modified timestamp (used to compute retention expiration date), and the checksum.

  - *Mutable* – storage class.

▶ For compliance with SEC 17a-4(f), a single, time-based retention rule called an *OSS Retention Strategy* with an appropriate retention period, must be (1) created and (2) locked for each Bucket that is intended to store regulated content. A Bucket's *OSS Retention Strategy* applies to all content in the Bucket.

1. An *OSS Retention Strategy* can be **created for a Bucket** by authorized users (or applications) via the OSS user console, SDKs or RESTful APIs.

   ◆ Versioning must be disabled for a Bucket before an *OSS Retention Strategy* is allowed.

   ◆ A retention period is required for the *OSS Retention Strategy*, ranging from 1 day to 70 years, and is stored as Bucket metadata. The retention period is applied to each record object's creation/storage date (Last Modified Date) to *calculate* the record object's protection period (retention expiration date). *Note: a retention expiration date is not stored as metadata for the record object itself.*

2. An *OSS Retention Strategy* and the associated retention period must be **locked,** via console, SDK or API, within 24 hours of creation to ensure compliance with the Rule.

   ◆ By default, each new *OSS Retention Strategy* is set to an initial <u>*InProgress*</u> state for up to 24 hours, during which time, all record objects within the Bucket are protected against modification, overwrites and deletion. **However, the OSS Retention Strategy may be deleted from the Bucket while in this <u>InProgress</u> state. If the OSS Retention Strategy is not locked within 24 hours, it will expire automatically, leaving contents of the Bucket unprotected.**

   ◆ Once the *OSS Retention Strategy* is locked, the following controls are enforced:

     ▪ Existing and new record objects within the Bucket are protected against modification and overwrites during their protection period. Versioning cannot be reenabled.

     ▪ Existing and new record objects within the Bucket cannot be deleted during their protection period.

     ▪ The retention period for the bucket's *OSS Retention Strategy* cannot be shortened, only extended.

     ▪ The *OSS Retention Strategy* for the Bucket cannot be deleted/removed.

     ▪ The Bucket itself cannot be deleted unless it is empty of all record objects (protected and unprotected).

▶ Record objects within a protected Bucket (i.e., a Bucket that has a locked *OSS Retention Strategy*):

● May be assigned to a new **storage class**. Such reassignment will not impact retention or immutability controls for the record object.

● Cannot be **moved** to another Bucket.

● May be **copied** to another Bucket. Retention and immutability controls will continue to apply to the original record object but will not be applied to its copy.

▶ Record objects that are uploaded to a protected Bucket, via a Multipart Upload operation, will only be protected once the entire multipart upload operation successfully completes. Should the operation fail, the uploaded fragments will not be protected and may be deleted by users.

▶ A record object may be appended once to the Bucket, after which no further append functions are allowed for that record object.

▶ If protected Buckets are copied to another Region, retention and immutability controls associated with the original Bucket will not apply to the copy.

Legal Hold

▶ When litigation or a subpoena requires record objects to be placed on hold, which could entail retaining them beyond their assigned retention period, the regulated entity must ensure the subject record objects are protected for the duration of the legal hold.

- A legal hold attribute can be set for a Bucket, via console, SDK or API, to "Yes/True" to preserve all record objects in the Bucket for purposes of subpoena, litigation, regulatory investigation, and other similar circumstances.

  - A legal hold can exist at the Bucket level as an independent control for the enclosed record objects; and therefore, does not require a Bucket to also have an assigned *OSS Retention Strategy*.

- All record objects stored within a Bucket, including those written to a Bucket after a legal hold is applied, will be protected against (a) deletes, (b) changes, (c) overwrites, and (d) versioning, while the legal hold attribute remains set for the Bucket.

- The legal hold attribute can be cleared (changed to "No/False") for the Bucket when no longer required; thereafter, immutability controls for the Bucket and its contents are once again governed by the Bucket's *OSS Retention Strategy*, if one exists.

Deletion Controls

▶ Record objects stored in a Bucket with a locked *OSS Retention Strategy* are protected from premature deletion by any source, including root accounts, during the protection period.

▶ Record objects become eligible for deletion when both of the following conditions are met:

1. The record object's retention expiration date is in the past, as calculated by adding the Bucket's retention period to the record object's creation/storage date (Last Modified Date). **Note: Once a record object has passed its retention expiration date, it is no longer immutable. However, should any modifications be made to the record object, its *Last Modified* timestamp will be updated, causing immutability and retention controls to immediately be reinstated.**

2. The legal hold attribute for the Bucket is set to "No/False."

▶ Eligible record objects may be deleted from storage via the OSS user console, SDKs or RESTful APIs. Alternatively, OSS *Lifecycle Deletion Rules* may be established to automatically delete eligible record objects, based on predefined criteria (e.g. the age of the record object).

- The OSS Lifecycle Delete process runs daily and computes eligibility for each record object covered by a *Lifecycle Deletion Rule*. Records found to be eligible for deletion are automatically removed from storage.

▶ *Buckets* that have a locked *OSS Retention Strategy* and/or a legal hold applied, are protected against deletion until all record objects are first deleted from the Bucket.

▶ Deletion of an Account that has one or more Buckets with locked *OSS Retention Strategies* is prohibited.

Clock Management

▶ The Object Storage Service utilizes a globally deployed NTP (Network Time Protocol) service on the Alibaba Cloud Platform to synchronize clocks across its servers to prevent, or immediately detect and correct, any inadvertent or intentional administrative modifications of the time clock. This process protects against premature deletion of retained record objects.

- OSS server clocks regularly synchronize with the NTP service.

- Detected synchronization discrepancies generate an alert and gradual resynchronization with the NTP service is immediately initiated.

Security

▶ The Alibaba Cloud Platform undergoes rigorous, third-party audits of security, privacy and compliance controls on a regular basis. For more information see https://www.alibabacloud.com/trust-center.

▶ The Object Storage Service supports all standard encryption services.

- HTTPs is recommended for transmission of record objects over the internet.

- Data at rest on OSS may be protected by server-side encryption, utilizing the provided KMS (key management system) or a KMS provided by the customer.

- Additionally, the Object Storage Service supports client-side encryption.

2.1.4   Additional Considerations

To assure compliance with the non-erasable and non-rewriteable requirements of the SEC Rule, the regulated entity is responsible for:

▶ Applying and locking an *OSS Retention Strategy*, with an appropriate retention period, to every Bucket that is used to store regulated record objects. If differing retention periods apply to record objects, the regulated entity must either (a) setup separate Buckets, each with an appropriate retention period or (b) set a retention period equal to the longest retention period associated with the retained record objects within the Bucket.

▶ Ensuring all record objects required to be retained for compliance with the SEC Rule are uploaded to a properly configured OSS Bucket; Cohasset recommends uploading to OSS within 24 hours of creation or storing in an SEC-compliant protected storage system until they are uploaded to OSS.

▶ Storing record objects requiring event-based[4] retention periods in a separate compliance system, since Alibaba Cloud Object Storage Service does not currently support event-based retention periods.

---

[4]   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.

▶ Applying legal holds to Buckets with record objects that require preservation for legal matters, government investigations, external audits and other similar circumstances, and clearing the legal holds when the applicable action is completed.

- Further, since legal holds apply to all contents of a Bucket, Cohasset recommends that the regulated entity contemplate the type of record objects stored in each Bucket to limit excessive preservation.

▶ Establishing appropriate security policies and procedures to:

- Restrict access to the OSS root account and define the actions of the OSS administrators.

- Ensure appropriate levels of encryption are enabled for record objects at rest and in transit.

- Ensure appropriate management of encryption keys, if utilizing client-side encryption.

- Periodically verify Alibaba's security/privacy/compliance audit results and/or certification reports.

▶ Properly maintaining their Alibaba account and paying for all appropriate services to ensure that protection of all record objects continue until their protection period has expired or until the record objects have been transferred to another compliant storage system.

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 Object Storage Service capabilities, in conjunction with the inherent capabilities of advanced magnetic storage technology, meet the requirements of the Rule.

2.2.3   Alibaba Cloud Object Storage Service Capabilities

The Object Storage Service has a combination of recording and post-recording verification processes, which are described in the following subsections.

Recording Process

▶ A combination of checks and balances in the advanced magnetic recording technology, such as inter-component and inter-step cyclical redundancy checks (CRCs), as well as write-error detection and correction, are relied upon to ensure that the records are written in a high-quality and accurate manner.

▶ To verify that no errors occur during transmission or the recording process, the Object Storage Service automatically calculates a checksum as part of the record object upload process. Additionally, checksums

calculated and transmitted with the record object by the client source application are supported. After the write process, checksum(s) are recalculated and compared to the original. If the checksums do not match, the write process fails, an error is returned to the user, and the record object must be resent by the source system.

- Checksums are retained as metadata for each record object for use during future retrievals and integrity verification.

Post-Recording Verification

▶ To validate continued data integrity, the Object Storage Service periodically scans data at rest to verify that recalculated checksums match stored values. In the event the checksums do not match, an accurate replica is automatically regenerated from a duplicate.

▶ During every read back of a record object, the Object Storage Service recalculates the checksum and compares it to the stored value to verify the integrity of the record object. In the event the checksums do not match, an accurate replica is automatically generated from a duplicate.

▶ When the Object Storage Service receives a download request, associated checksums are automatically transmitted with the record object for client-side validation.

2.2.4   Additional Considerations

▶ When storing a record object, Cohasset recommends that the client/user application send a checksum to confirm the transmission of the record object.

▶ For retrieval, Cohasset recommends that the client/user application request that a checksum be transmitted with the record object, for validation of the transmission.

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

It is Cohasset's opinion that the capabilities of the Object Storage Service meet the requirements of the rule for serializing the original and duplicates of the record objects.

2.3.3   Alibaba Cloud Object Storage Service Capabilities

▶   Each record object is assigned a unique, internal identifier that is immutable and guarantees uniqueness within the Object Storage Service environment. In addition, the client provides a combination of the following immutable attributes:

- The <u>Bucket name</u> must conform to Object Storage Service's naming standards and be globally unique within the Object Storage Service.

- The <u>record object name</u> (Key) must conform to Object Storage Service's naming standards and be unique within the Bucket.

▶   System-generated creation/storage date and time (Last Modified timestamp) is recorded as system metadata for the Object and is immutable during the protection period.

▶   The combination of (a) the unique identifiers (Alibaba internal identifier and client-provided Bucket and record object names) and (b) Last Modify timestamp, serializes 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 the capabilities of the Object Storage Service meet the requirements of the Rule by providing the capabilities to (a) create a list of record objects and associated metadata and (b) select and download all or part of the list. Thereafter, local capabilities may be used to transfer the record object to a medium acceptable under the Rule.

2.4.3   Alibaba Cloud Object Storage Service Capabilities

Capabilities that support the capacity to download record objects and metadata include:

▶   From the OSS user console, authorized users may perform searches based on file names or browse through the names of all files (record objects) that are contained within a selected Bucket. Further, record objects may be listed in lexicographic order, using the pseudo folders to structure the list. Once files are located:

- The contents may be viewed in a browser. If the contents are not compatible with a browser, the file will automatically be downloaded to the client when the URL is opened.

- The file's URL may be shared with other authorized users so that they may view and download the file.

- One or more files may be selected for download to a local system.

The requested records are retrieved and sent to the client/user application where they may be viewed and reproduced or transferred to a medium acceptable under the Rule.

▶ Additionally, via API calls, a list of selected, or all record objects stored in a Bucket, can be requested.

- The results of the API call will include the Bucket and record object names and metadata for record objects matching the API parameters.

- No *OSS Retention Strategy* attributes (i.e. retention period) are returned with the list.

Once the list of record objects and metadata is available, other API's may be used to download one or more record objects. Once the record objects have been retrieved, local client/user application capabilities may be used to view, reproduce or transfer the record objects to a medium acceptable under the Rule.

2.4.4   Additional Considerations

The regulated entity is responsible for submitting the downloaded record objects and index metadata to the SEC or designated SRO/DEA, as requested.

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 the current capabilities of the Object Storage Service meet the requirements of the Rule by utilizing erasure coding, which stores coded segments of the record object across multiple storage devices in multiple Availability Zones, allowing an accurate replica to be generated, if an error occurs. Optionally, Cross-Region Replication is available to provide geographically-dispersed replication of record objects.

2.5.3   Alibaba Cloud Object Storage Service Capabilities

▶ The Object Storage Services redundantly stores record objects within a Region for durability and availability purposes. Erasure coded segments of the record object are stored across multiple storage devices located in multiple Availability Zones. In the event of an error, an accurate replica of the complete record object can be regenerated.

- The Object Storage Service is designed to provide 11 nines of durability (i.e., 99.999999999% reliable) for data stored in a single Region. This means that stored objects are highly protected against loss from data corruption caused by underlying media failures.

▶ Optionally, Cross-Region Replication is available to provide geographically-dispersed replication of data. Should services in the primary Region become unavailable, an Account with Cross-Region Replication enabled can immediately be switched over to the backup Region.

▶ The Object Storage Service automatically recovers record objects when (a) the checksum recalculated during a read back or background integrity check indicates an has error occurred with a replica of a stored record object or (b) errors on one or more storage devices within a Region are detected.

2.5.4 Additional Considerations

There are no additional considerations related to this requirement.

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 Alibaba Cloud Object Storage Service, utilized with the OSS Retention Strategy feature, 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 SEC 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 <u>integrated</u> hardware and software <u>control codes</u>.* [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 Alibaba Object Storage Service, utilized with the OSS Retention Strategy feature, 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:*
> <u>Electronic regulatory records</u> *means all regulatory records other than regulatory records exclusively created and maintained by a records entity on paper.*
> <u>Records entity</u> *means any person required by the Act or Commission regulations in this chapter to keep regulatory records.*
> <u>Regulatory records</u> *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, <u>with respect to such books and records stored electronically, regulatory records shall also include:</u>*
> <u>*(i) Any data necessary to access, search, or display any such books and records; and*</u>
> <u>*(ii) All data produced and stored electronically describing how and when such books and records were created, formatted, or modified*</u>. [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 Alibaba Object Storage Service, with a locked *OSS Retention Strategy,* 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 of the Alibaba Object Storage Service, as 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 Alibaba Object Storage Service, when utilized with locked _OSS Retention Strategies_, retains immutable metadata (index attributes) as an integral part of the 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 (Last Modified) date and time, and object checksums. Additionally, mutable (changeable) metadata attributes stored for a record object include the assigned storage class. 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 [5] 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 Alibaba Cloud Object Storage Service 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 the Object Storage Service by utilizing erasure coding, which stores coded segments of the record object across multiple storage devices in multiple Availability Zones, allowing an	_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)]

---

[5] 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
	accurate replica to be generated, if an error occurs. Optionally, Cross-Region Replication is available to provide geographically-dispersed replication of record objects. To satisfy this requirement for <u>other</u> 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 Alibaba Cloud Object Storage Service 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 the use of the Alibaba Object Storage Service to retrieve and download the record objects and the associated metadata retained by the Object Storage Service utilized with the *OSS Retention Strategy* feature. 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 Alibaba Cloud Object Storage Service with the *OSS Retention Strategy* feature, 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 Alibaba Cloud Object Storage Service with the *OSS Retention Strategy* feature.

Cohasset determined that Alibaba Cloud Object Storage Service, when utilized with **_locked_ OSS Retention Strategies,** 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 time-based[6] retention periods.

- Preserves all record objects in a Bucket as immutable and prohibits deletion or overwrites, while a Legal Hold attribute is applied.

- Prohibits *deletion* of a record object and its immutable metadata until the retention period for the record object, and any Legal Hold on the Bucket, has expired.

- Supports server-side and client-side encryption of record objects.

- Verifies the accuracy and quality of the recording process automatically using advanced storage recording technology and checksums to validate the initial recording process and for automatic post recording integrity verifications.

- Redundantly stores record objects across multiple storage devices located in multiple Availability Zones for durability and availability and regenerates an accurate replica of the complete record object from erasure coded segments, in the event of an error.

- Uniquely identifies and chronologically serializes each stored record object.

- Allows authorized users and applications to access record objects and metadata via OSS user console, SDKs or RESTful APIs, for local reproduction or transfer to a format and medium acceptable under the Rule.

Accordingly, Cohasset concludes that the Alibaba Cloud Object Storage Service, when utilized with locked *OSS Retention Strategies* to retain time-based records, meets the requirements that relate directly to the recording, storage and retention of record objects and system metadata.

---

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

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 SEC Rules 17a-3 and 17a-4, when the system delivers the prescribed functionality. Specifically, SEC 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 <u>meets the applicable conditions set forth in this paragraph (f)</u>. [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. <u>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.</u> 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

***<u>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.</u> 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.[7] [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 <u>integrated</u> hardware and software <u>control codes</u>. [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).

---

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

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:

> *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 *five* SEC requirements relevant to the recording, storage and retention of electronic records and a description of the capabilities of the Alibaba Cloud Object Storage Service 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 [Securities Exchange Act] 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, <u>principles-based approach</u>, proposed § 1.31(d)(1) would <u>rephrase the existing requirements in the form of a general standard</u> for each records entity to retain all regulatory records in a form and manner necessary to <u>ensure the records' and recordkeeping systems' authenticity and reliability</u>. 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.

<u>Electronic regulatory records</u> means all regulatory records other than regulatory records exclusively created and maintained by a records entity on paper.
<u>Records entity</u> means any person required by the Act or Commission regulations in this chapter to keep regulatory records.
<u>Regulatory records</u> 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, <u>with respect to such books and records stored electronically, regulatory records shall also include:</u>
<u>(i) Any data necessary to access, search, or display any such books and records; and</u>
<u>(ii) All data produced and stored electronically describing how and when such books and records were created, formatted, or modified.</u> [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[8] and event-time-based[9] 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, <u>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</u>.
(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 <u>one year from the date of such communication</u>.
(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 <u>five years from the date on which the record was created</u>. [emphasis added]

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

---

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

9   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.