Cohasset Associates

SEC 17a-4(f), FINRA 4511(c) & CFTC 1.31(c)-(d) Compliance Assessment

Amazon Web Services (AWS) Simple Storage Service (S3)

Abstract

Amazon Web Services ("AWS") is a secure cloud services platform hosted by Amazon to provide modular cloud-based products and services. Amazon Simple Storage Service ("S3") is an AWS service that provides cloud-based object storage that is designed to provide scalability, high availability, and low latency.

In this Report, Cohasset Associates, Inc. ("Cohasset") assesses the functionality of Amazon S3 relative to the recording, storage, and retention requirements for electronic records 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 Amazon S3, when properly configured and when *Object Lock* mode is set to *Compliance*, retains time-based records in non-erasable and non-rewriteable format and meets the 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.

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[2] 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 Amazon Web Services ("AWS") Simple Storage Service ("S3"), when the Object Lock mode is set to Compliance, 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, AWS engaged Cohasset to complete an independent and objective assessment of the capabilities of Amazon S3, when the Object Lock mode is set to Compliance, 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 Amazon S3.*

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, 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).

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 Amazon S3, 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 Amazon S3, in comparison to relevant storage-specific requirements set forth in SEC Rule 17a-4(f) and CFTC Rule 1.31(c)-(d), Amazon Web Services ("AWS") 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 Amazon S3 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 Amazon S3; 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.

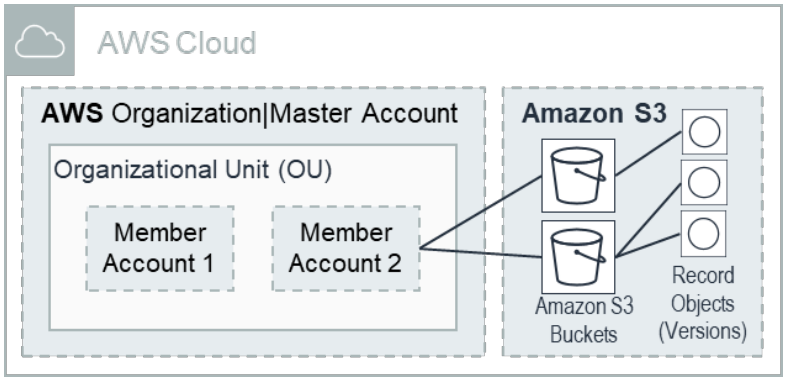
This assessment represents the professional opinion of Cohasset and should not be construed as either an endorsement or a rejection, by Cohasset, of Amazon S3 and its capabilities or other AWS products or services. The information utilized by Cohasset to conduct this assessment consisted of: (a) oral discussions, (b) system documentation, (c) user and system administrator guides, and (d) other directly-related materials provided by AWS 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 Amazon S3 Overview

Amazon Web Services ("AWS") is a secure cloud services platform hosted by Amazon to provide modular cloud-based products and services. AWS offers compute power, data storage, content delivery and other functionality. Amazon Simple Storage Service ("S3") is an AWS service that provides cloud-based object storage that is designed to provide scalability, high availability, and low latency.

The hierarchy of these AWS services is summarized as follows:



- An Organization has one AWS **Master Account** and it may have multiple Organizational Units to group its AWS Member Accounts.
- **Organizational Units** may be nested, allowing **Member Accounts** to be hierarchical and managed centrally.
- A **Member Account** is assigned to one Organization Unit at a time and may have multiple Amazon S3 Buckets, as one of its services.
- **Amazon S3** is the storage infrastructure. **Buckets** are public cloud storage resources available in Amazon S3 storage services. Amazon S3 Buckets retain individual versions of objects (hereinafter "**record objects**"), which are comprised of the content and its descriptive metadata. Record objects are identified within each bucket by a unique, user-assigned key, and version identifier.
- **Identity and Access Management (IAM) policies** apply roles to users.

This assessment report focuses on Amazon S3 Buckets and stored record objects when the *Object Lock* mode is set to *Compliance* and an appropriate retention period is applied. The *Compliance* setting is designed to meet the SEC Rule 17a-4(f) requirements, to preserve electronic record objects as non-rewriteable, non-erasable for the required retention period and any applied legal hold.

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

This section presents Cohasset's assessment of the capabilities of Amazon S3 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 Amazon S3
- ***Amazon S3 Capabilities*** – Description of relevant capabilities of Amazon S3
- ***Additional Considerations*** – Additional considerations related to meeting the specific requirement

The following subsections document Cohasset's assessment of the capabilities of Amazon S3, 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)]

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

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]."*

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 capabilities of Amazon S3 meet the requirements of the Rule for managing records requiring time-based[3] retention, as non-rewritable and non-erasable for the applied retention period and preservation for legal holds, when Amazon S3 and Bucket features are properly configured and utilized to retain individual versions of record objects[4], and appropriate retention controls are applied (i.e., *Retain Until Date* is set to the appropriate retention expiration date and the *Object Lock* mode is set to *Compliance*), and the considerations identified in Section 2.1.4 are satisfied.

2.1.3 Amazon S3 Capabilities

In this subsection, Cohasset presents the capabilities of Amazon S3 that directly pertain to the SEC Rule 17a-4(f) requirement for preserving electronic records (record objects) in a format that is non-rewritable and non-erasable, for the required retention period and any associated legal holds.

2.1.3.1 General Information

Each customer's **Organization** has one designated **Master Account** and may have one or more Member Accounts, which are connected to Amazon S3 Bucket(s). The Amazon S3 provides the storage services for record objects and associated metadata on the AWS cloud infrastructure.

To meet this SEC Rule 17a-4(f) requirement:

- *Versioning* and the Amazon S3 **Object Lock feature** must be enabled (On) for the Amazon S3 Bucket.
- For each record object stored in the Amazon S3 Bucket, an appropriate *Retain Until Date* must be applied and the ***Object Lock* mode** must be set to *Compliance*.
- The *Legal Hold* status for a record object may be enabled, as needed, to suspend eligibility for deletion of the record object until the *Legal Hold* status is cleared.

  REMINDER: Each version is an independent record object; accordingly, the *Retain Until Date, Object Lock* mode, *Legal Hold* status, must be applied to each version, as required for compliance.

[3] Time-based retention periods require the Blob (record) to be retained for a fixed, contiguous period of time calculated from the date the object is created/stored.

[4] In this report, the term *record object* refers to each distinct version of an object and is used to reflect that certain files are *books and records* that are required to be maintained for a specific period of time (the retention period), as stated in regulations, such as SEC Rules 17a-3 and 17a-4 and CFTC Rule 1.31.

The fundamental features of Amazon S3 prevent changes or modifications to record objects or its immutable metadata, once stored. Further, with the above configurations and settings:

- The record object, and its immutable metadata, cannot be overwritten or deleted until both the applied *Retain Until Date* has expired and the record object *Legal Hold* status is cleared.
  - These settings prevent all (a) user-initiated actions, via AWS and Amazon S3 management consoles, Amazon S3 API (application program interface), and the AWS CLI (command-line interface), as well as (b) lifecycle policies from overwriting or deleting the record object before the *Retain Until Date* has expired.
- Further, the *Object Lock* mode must be set to *Compliance*, which ensures that the *Retain Until Date* cannot be shortened or removed, disallowing premature deletion.

These features and protections apply across all Amazon S3 storage classes, including Amazon Glacier[5] (archival storage). Therefore, lifecycle policies may be used to tier record objects into Amazon S3 storage classes.

2.1.3.2 Amazon S3 Bucket Configurations

- For each Amazon S3 Bucket that will retain record objects required to comply with SEC Rule 17a-4(f), *Versioning* and the Amazon S3 **Object Lock feature** must be enabled (On). Once set for a Bucket, these two configurations cannot be suspended or disabled.
- Optionally, a pair of Bucket defaults – *Default retention period* (e.g., 6 Years) together with ***Object Lock* mode** (e.g., *Compliance*) – may be configured to automatically apply retention controls to each stored record object, unless retention controls are explicitly transmitted with the record object.
  - The *Default retention period* is added to the creation/storage date to calculate the record object's *Retain Until Date*. (See section 2.1.3.3, *Record Object Definition and Retention Controls*, for more information.)
  - The *Object Lock* mode settings include both *Compliance* and *Governance*.
    - IMPORTANT NOTE: The *Object Lock* mode must be set to *Compliance*, for record objects required for compliance with SEC Rule 17a-4(f), which disallows all users, including the account root user, from shortening or removing the *Retain Until Date*.
  - Authorized users may change the Bucket default values at any time, including: (a) shortening the *Default retention period*, (b) changing the default *Object Lock* mode between *Governance* and *Compliance,* or (c) clearing (removing) both default values. The updated default values apply day-forward and do not apply to previously stored record objects; therefore, previously applied object-level protections remain unchanged.
- Optionally, *Minimum and Maximum retention periods* (Min/Max range) may be configured using AWS Identity and Access Management (IAM). IAM roles define a set of permissions that grant access to actions and resources in AWS. For example, an IAM Role is defined and permissioned to apply retention periods between

[5] The Amazon S3 *Object Lock* feature is in addition to the previously released Amazon Glacier *Vault Lock* feature for preserving record objects in a non-rewritable and non-erasable format.

[Minimum] and [Maximum] period. The IAM Role is applied to users (e.g., source applications) permissioned to store record objects in the Bucket.

- Since the *Minimum and Maximum retention periods* are set through IAM, each permissioned user of a Bucket may be bound by a different Min/Max range.
  - Authorized users may change the Min/Max range at any time. The updated Min/Max range applies day-forward and does not apply to previously stored record objects.
- When a record object is stored, if the *Retain Until Date* is outside the Min/Max range for the user, the record object will be rejected, and an error will be reported. Therefore, the *Default retention period* must be set between the Min/Max range applied to users authorized to store objects in the Bucket.

2.1.3.3 Record Object Definition and Retention Controls

- Each record object has a separate *Retain Until Date* and *Object Lock* mode. (REMINDER: The term record object is defined as a version of a record object.) Each record object is comprised of:
  - The complete content of the record object.
  - Immutable metadata, which includes, but is not limited to, unique object key name, version identifier, creation/storage date (last modified date) and object size, and user-defined custom metadata (key-value pairs).
  - Mutable metadata, which includes, but is not limited to, retention controls (*Retain Until Date* and *Object Lock* mode), Amazon S3 access control lists (ACLs), and Amazon S3 tags.
- The *Object Lock* mode can be set to one of three options for a given record object; **only** *Compliance* mode meets the requirements of SEC Rule 17a-4(f).
  1. *Object Lock* mode set to *Compliance,* assures the following retention controls:
     - The *Retain Until Date* may be extended to a future date but cannot be shortened or cleared, by any user, including the account root user.
     - The *Compliance* setting for the *Object Lock* mode cannot be changed to *Governance* or cleared by any user, including the account root user.
  2. *Object Lock* mode set to *Governance,* permits shortening or clearing the *Retain Until Date,* as well as clearing the *Object Lock* mode. As a result, *Governance* mode is disallowed for records required to comply with the Rule.
  3. *Object Lock* mode may be *blank (null),* which does not apply any retention protections.
- The following Amazon S3 features prevent modification, overwrite and deletion, until eligible.
  - The fundamental capabilities of Amazon S3, immutably stores record objects and certain metadata.
  - The *Versioning* feature ensures that objects are not overwritten, and instead a new version is created.
  - Each record object is protected from deletion, by users and by lifecycle policies, when either:

- The *Retain Until Date* of the record object is a future date (not in the past), or
- The *Legal Hold* status of the record object is set.

- To apply a *Retain Until Date* and *Object Lock* mode of *Compliance* to the record object that is required by regulation:
  1. The source application may transmit an explicit *Retain Until Date* and *Object Lock* mode of *Compliance* with a record object.
  2. If the record object is transmitted *without* retention values, the Bucket *Default retention period* is added to the storage date to calculate the *Retain Until Date* and default *Object Lock* mode is applied to the record object. Accordingly, for compliance with the Rule, the default *Object Lock* mode must be set to *Compliance*.
     - Considering the automatic application of Bucket defaults, Cohasset recommends setting a Bucket *Default retention period* and default *Object Lock* mode of *Compliance* for Buckets used to store records required by the Rule. This assures that retention controls are applied to *all* record objects stored in the Bucket.
     - If Bucket defaults are not configured, the record object is transmitted *without* retention values, it is stored without retention controls.
- The retention controls for previously stored record objects may be updated. For record objects previously stored with its *Object Lock* mode set to *Compliance:*
  - The *Retain Until Date* may be extended to a future date but cannot be shortened or cleared, by any user, including the account root user.
  - The *Compliance* setting for the *Object Lock* mode cannot be changed to *Governance* or cleared by any user, including the account root user.
- A record object may be copied between Amazon S3 Buckets, resulting in the creation of a new copy with its own unique metadata, including the assignment of a new *Retain Until Date*, *Object Lock* mode and *Legal Hold* status. The original record object and its metadata will remain, unaltered, in the original Bucket.
- A record object cannot be moved between Amazon S3 Buckets, unless the record object is eligible for deletion. If the record object is eligible for deletion, the move results in deleting the record object in the existing Bucket and creating a new record object in the new Bucket, with new metadata, including key name, version identifier, and creation/storage date.
- If the user does not have the required permissions or the user attempts the following, an error is logged, and the action is rejected:
  - Assign either a *Retain Until Date* or *Object Lock* mode. These attributes are a pair, and both must be specified, or both must be blank (null).
  - Shorten or remove a record object's *Retain Until Date* when the *Object Lock* mode is set to *Compliance*.
  - Set a *Retain Until Date* that is not within the *Minimum and Maximum retention periods* applied to the user through IAM policies.

- Change the *Object Lock* mode from *Compliance* to *Governance* or from *Compliance* to blank (null).
- Delete a record object before the *Retain Until Date* has passed (expired).
- Move a record object from a Bucket with the Amazon S3 *Object Lock* feature enabled (On).
- Disable (attempt to change to Off) the Amazon S3 *Object Lock* feature for the Bucket.

- To verify the retention controls for record objects either (a) view the metadata for the object or (b) run an inventory report for the Amazon S3 Bucket. For users with appropriate permissions the current *Retain Until Date* and *Object Lock* mode for each record object will be retrieved.

2.1.3.4 Legal Holds

- The *Legal Hold* (On/Off) status may be applied to any record object stored in a Bucket with the Amazon S3 ***Object Lock* feature** enabled (On). (REMINDER: The term record object is defined as a version of a record object.)
  - Each record object includes a separate *Legal Hold* status attribute.
  - The *Legal Hold* status is independent of the record object's *Retain Until Date* and *Object Lock* mode; therefore, a *Legal Hold* status may be applied to any record object in a Bucket with the Amazon S3 *Object Lock* feature enabled (On), including record objects without a *Retain Until Date* and *Object Lock* mode.
  - When the *Legal Hold* status is set (On), it prohibits overwriting and deleting the record object until the *Legal Hold* status is cleared (Off). Accordingly, this feature may be used to preserve a record object for subpoena, litigation, regulatory investigation and other special circumstances.
  - When the *Legal Hold* status is cleared (Off), this attribute no longer mandates preservation of the record object; however other retention controls continue to apply to the record object.
- If the user does not have the required permissions, an error is logged, and the action is rejected.
- To verify the *Legal Hold* status for a record object either (a) view the metadata for the object (e.g., *GetObjectLegalHold)* or (b) run an inventory report for the Amazon S3 Bucket. For users with appropriate permissions the current *Legal Hold* status for each record object will be retrieved.

2.1.3.5 Deletion

- The *Retain Until Date* and *Legal Hold* status determine if the record object is eligible for deletion (eligibility for deletion does not cause automatic deletion). The following criteria must be met for a record object to be eligible for deletion:
  - The *Legal Hold* status must be clear (Off).
  - The *Retain Until Date* must have expired (must have passed).
- An error is logged, and the action is rejected if the user does not have the required permissions or the user attempts to delete a record object when (a) the *Retain Until Date* has not passed or (b) the *Legal Hold* status is set (On).

- A Lifecycle Policy may be configured to automatically delete record objects. Only record objects that are eligible for deletion will be deleted.
- The Amazon S3 Bucket cannot be closed or deleted, until the Bucket is empty.

2.1.3.6 Clock Management

To meet the requirements of the Rule, Cohasset asserts that every system clock must synchronize to an external time server, e.g., a network time protocol (NTP) clock. The Amazon S3 system clocks regularly and frequently check the time of the external source and resynchronize. Neither end users nor system administrators have the ability to manipulate system time on Amazon S3. These controls prevent or correct any inadvertent or intentional administrative modifications of the time clock, which could allow for premature deletion of record objects.

2.1.3.7 Security

- Amazon Web Services are designed to meet Enterprise security and compliance requirements.
- Record objects and metadata are encrypted:
  - Optionally, data in-transit (data traveling to and from Amazon S3) may be protected using Secure Sockets Layer (SSL) or by client-side encryption.
  - Amazon S3 offers options for protecting data at rest (data stored on disks in Amazon S3 data centers):
    - **Server-Side Encryption** – Amazon S3 encrypts record objects before each is stored in its data centers and decrypts each record object it when downloaded. Amazon S3 offers three mutually exclusive options for managing encryption keys:
      - **Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)** – Each object is encrypted with a unique key employing strong multi-factor encryption. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates.
      - **Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)** – This feature is similar to SSE-S3, with added protection against unauthorized access of objects in S3 and an audit trail showing when the key was used and by whom. Additionally, encryption keys may be created and managed by the client.
      - **Server-Side Encryption with Customer-Provided Keys (SSE-C)** – The client manages the encryption keys and Amazon S3 manages the encryption, as it writes to disks, and decryption, when objects are accessed.
    - **Client-Side Encryption** – The regulated entity may encrypt data before uploading it to Amazon S3 for storage. With this option, the regulated entity manages the encryption process, the encryption keys, and related tools.
  - Roles-based Security (RBAC) is employed by AWS. The permissions for each user are controlled through IAM roles created for the client organization.

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:

- Appropriately assigning permissions required to manage the retention controls and properly configuring the Identity and Access Management (IAM) roles and Amazon S3 Buckets that will retain regulated records.
- Applying the retention controls to each record object that is required for regulatory compliance. (REMINDER: The term record object is defined as a version of a record object.) Cohasset recommends these controls be applied within 24 hours of storing the record object. This includes:
  - Applying a *Retain Until Date* that meets regulatory retention requirements, and
  - Setting the *Object Lock* mode to *Compliance*.

  NOTE: Cohasset recommends configuring an appropriate *Default retention period* and a default *Object Lock* mode of *Compliance* for Buckets that will store record objects required for compliance with SEC Rule 17a-4(f). These defaults will assure that all record objects are stored with retention controls.
- Setting a *Legal Hold* status to On, as needed, to preserve record objects for legal matters, government investigations, external audits and other similar circumstances, and setting the *Legal Hold* status to Off, when preservation is no longer required.
- Storing record objects requiring event-based[6] retention periods in a separate compliance system, since Amazon S3 does not currently support event-based retention periods.

Optionally, the regulated entity may set *Minimum and Maximum retention periods* in an IAM policy to validate the *Retain Until Date* applied to each record object.

To verify that the *Retain Until Date*, *Object Lock* mode and *Legal Hold* status are applied to each record object the regulated entity may view attributes by (a) retrieving the metadata attributes for each record object, or (b) running an inventory report for the Bucket.

Additionally, the regulated entity is responsible for (a) maintaining their AWS Master Account, (b) paying for appropriate services, and (c) procedurally prohibiting users from closing Member Accounts until either (1) the retention periods have expired on record objects stored in the associated Buckets or (2) until the record objects have been transferred to another compliant storage system. Similar to decommissioning infrastructure, closing a Master Account or a Member Account will delete the associates Amazon S3 Buckets and record objects, even if the record object is *not* eligible for deletion.

[6] 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. Both the SEC and CFTC have defined recordkeeping obligations that require event-based retention periods.

2.2 Accurate Recording Process

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

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

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.

2.2.2 Compliance Assessment

It is Cohasset's opinion that Amazon S3 capabilities, related to the data recording process and the post-recording verification, meet the requirements of the Rule.

2.2.3 Amazon S3 Capabilities

The recording and the post-recording verification processes of Amazon S3 are described below.

2.2.3.1 Recording Process

- An MD5 checksum must be transmitted with the record object, if a *Retain Until Date* and *Object Lock* mode are applied, either explicitly transmitted with the record object or inherited by the *Default retention period* for the Bucket. The record object will be stored only if the MD5 checksum value calculated by Amazon S3 matches the uploaded checksum. If it does not match, an error is reported, and the record object must be re-uploaded.
  - If a record object is stored without retention controls and the *Retain Until Date* and *Object Lock* mode are applied at a later time, an MD5 checksum is not required.
- Amazon S3 utilizes advanced electronic recording technology which applies a combination of checks and balances to assure that record objects are written in a high quality and accurate manner.

2.2.3.2 Post-Recording Verification Process:

- Standard Amazon S3 storage is designed to provide 99.999999999% durability and 99.99% availability of objects over a given year.
- Amazon S3 regularly verifies the integrity of data stored using checksums. If Amazon S3 detects data corruption, it is repaired using redundant data.
- Amazon S3 also calculates checksums on all network traffic to detect corruption of data packets when storing or retrieving data.

2.2.4 Additional Considerations

For retrieval, Cohasset recommends that the source application request the MD5 checksum for the record object and use it to validate transmission of the downloaded record object.

2.3 Serialize the Original and Duplicate Units of Storage Media

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

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.

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."*

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 Amazon S3 meet this SEC requirement to serialize the original and duplicate record objects.

2.3.3 Amazon S3 Capabilities

- Each record object is serialized in Amazon S3 Buckets using a combination of: (a) a unique Object Key Name (which includes Bucket name, prefix and object name) and (b) version identifier. These attributes are immutable.
  - The Bucket name must be globally unique across Amazon S3.
  - The object name must be unique within the Bucket.
  - The version identifier is automatically incremented.
- The creation/storage date (last modified date) is system-defined, immutable, and stored with each record object.
  - When the *Default retention period* is used, the record object creation/storage date is added to the *Default retention period* to calculate the *Retain Until Date* for the record object.
- This combination of Object Key Name, version identifier, and creation/storage date 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 Amazon S3 meets this SEC requirement by: (a) maintaining hardware and software capacity and high data availability, and (b) providing capabilities for an administrator or source application to select and download record objects and metadata (index) attributes. These record objects and metadata (index) attributes can then be transferred, by the regulated entity, in the format and media requested for production.

2.4.3 Amazon S3 Capabilities

Record objects and metadata (index) attributes may be downloaded using the Amazon S3 API, CLI or Management Console. The following capabilities support the capacity to download record objects and metadata (index) attributes:

- AWS assures that hardware and software capacity allows for ready access to the record objects and metadata (index) attributes. Further, AWS maintains redundant storage media, network, and power to mitigate outages that would result in unavailability of data.
- Using the Amazon S3 API, CLI or Management Console, authorized users can:
  - Run an inventory report for a specific Bucket and list record objects in lexicographic order.
  - List record objects in a Bucket (selection criteria may be defined to find and return a subset of the objects in a Bucket).
  - Search for an object using the Object Key Name and version identifier.
  - Download selected record objects and the associated metadata (index) attributes to a designated storage location.

  For each of the above actions, based on user permissions, certain metadata will be returned, including Object Key Name, version identifier, creation/storage date, *Retain Until* date, *Object Lock* mode, and *Legal Hold* status for each record object.
- When multiple versions of a record are stored, the top-level version is returned, by default. The specific version identifier must be specified in the search and download requests.

2.4.4 Additional Considerations

The regulated entity is responsible for (a) maintaining its account in good standing, (b) authorizing user permissions, (c) maintaining hardware and software to access AWS and Amazon S3, (d) maintaining Client-Side Encryption keys used in addition to the AWS Server-Side Encryption keys, and (e) assuring that the regulator, self-regulatory organization or designated examining authority receive downloads of the requested versions of the record objects and associated metadata (index) attributes, in the requested format 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

Cohasset believes that Amazon S3 meets this SEC requirement by providing a highly durable storage infrastructure designed such that record objects are redundantly stored on multiple devices across multiple facilities in an AWS region.

2.5.3 Amazon S3 Capabilities

- Amazon S3 redundantly stores record objects on multiple devices across multiple facilities in an AWS region. When a record object is uploaded to Amazon S3, data is synchronously stored across multiple facilities before a *success* response is returned.
- Standard Amazon S3 storage is:
  - Backed by the Amazon S3 Service Level Agreement.
  - Designed to provide 99.999999999% durability and 99.99% availability of objects over a given year.
  - Designed to sustain the concurrent loss of data in two facilities.
- Buckets, with the Amazon S3 *Object Lock* feature enabled, are **not** currently supported as a source, but are supported as a target, for Cross-Region Replication (CRR). When used as a target, the target's *Default retention period* and default *Object Lock* mode will be applied to replicated record objects.

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 Amazon S3, when properly configured and when *Object Lock* mode is set to *Compliance*, in comparison the principles-based requirements of CFTC Rule 1.31(c)-(d).

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 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 Amazon S3, as described in Section 2, 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 Amazon S3, when *Object Lock* mode is set to *Compliance*, 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 Amazon S3, 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 Amazon S3, when *Object Lock* mode is set to *Compliance*, retains certain 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 key name, creation/storage (last modified) date, MD5 checksum and user-defined custom metadata (key-value pairs). Additionally, mutable (changeable) metadata attributes stored for a record object include retention controls, *Legal Hold* status, Amazon S3 access control lists (ACLs), and Amazon S3 tags. 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 Amazon S3, 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 by Amazon S3.	*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
	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 Amazon S3, when *Object Lock* mode is set to *Compliance*, 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 Amazon S3 to retrieve and download the record objects and the associated metadata retained in Amazon S3 Buckets. 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 Amazon S3, when *Object Lock* mode is set to *Compliance*, 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 Amazon S3, as described in Section 2 of this report.

Cohasset determined that Amazon S3, when *Object Lock* mode is set to *Compliance*, has the following capabilities, which support its ability to meet the recording, storage and retention requirements:

- Maintains record objects and certain record object metadata in a non-erasable and non-rewriteable format for time-based[8] retention periods, when a *Retain Until Date* is applied and the *Object Lock* mode is set to *Compliance*.
- Allows a *Legal Hold* status 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 applied *Retain Until Date* has expired.
- Encrypts record objects data at rest (data stored on disks in Amazon S3 data centers), by default; and, supports encryption of data in-transit (data traveling to and from Amazon S3) using SSL (Secure Sockets Layer) or by client-side encryption.
- Verifies the accuracy and quality of the recording process automatically utilizing (a) advanced storage recording technology and (b) an MD5 checksum that must be received from the source system, if retention controls are applied to the record object during the recording process. The MD5 checksum 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 Amazon S3 API, CLI or Management Console 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 redundant objects, should data be lost or damaged.

Accordingly, Cohasset concludes that Amazon S3 meets the requirements that relate directly to the recording, storage and retention of record objects and system metadata, when the Amazon S3 Buckets are properly configured and utilized to retain time-based records, the *Object Lock* mode is set to *Compliance* and the *Retain Until Date* meets regulatory requirements.

[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.

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 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.*[9] [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).

[9] 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 the *five* SEC requirements relevant to the recording, storage and retention of electronic records and a description of the capabilities of Amazon S3 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, 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[10] and event-time-based[11] 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 AWS S3 in relation to each requirement, see Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*.

[10] 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.

[11] 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.

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*

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

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

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.