Cohasset Associates

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

Dell EMC Elastic Cloud Storage (ECS)

Abstract

BENEFIT FROM COHASSET'S INDUSTRY INSIGHT AND EXPERIENCE

Cohasset's primary business focus is to provide records management and information governance consulting and educational services to regulated organizations, including the financial services industry. These services align information lifecycle controls with business priorities, resulting in ongoing regulatory compliance, effective risk mitigation and measurable business efficiencies for domestic and multi-national clients.

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

Dell EMC® Elastic Cloud Storage (ECS™) is a cloud-based, object storage appliance where the storage control software and the physical magnetic disk media are combined as an integrated system with no access to the storage media other than through ECS. ECS is an append-only virtual storage platform that protects content from being erased or overwritten for a specified retention period.

In this Assessment Report, Cohasset Associates, Inc. (Cohasset) assesses the functionality of ECS relative to the storage requirements of the:

- Securities and Exchange Commission (SEC) in regulation 17 C.F.R. § 240.17a-4(f), which regulates exchange members, brokers or dealers.
- Commodity Futures Trading Commission (CFTC) in regulation 17 C.F.R. § 1.31(b)-(c), which regulates commodity futures trading.

It is Cohasset's opinion that ECS version 3.0, when Compliance is enabled for a Namespace and when properly configured and utilized to store and retain records in non-erasable and non-rewriteable format, meets the relevant storage requirements of SEC Rule 17a-4(f), CFTC Rule 1.31(b)-(c), and FINRA Rule 4511 which defers to SEC Rule 17a-4.

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) and the Commodity Futures Trading Commission (CFTC) define rigorous and explicit requirements for organizations that elect to retain books and records on electronic storage media.

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

The Dell EMC Elastic Cloud Storage ("ECS"), when Compliance is enabled for a Namespace, was designed to meet the stringent electronic records requirements for the receipt, storage and retention of regulated books and records. To evaluate its compliance with the SEC and CFTC requirements, Dell EMC engaged Cohasset to complete an independent and objective assessment of the capabilities of the ECS version 3.0 with Compliance enabled, relative to meeting these requirements.

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

1.1 Overview of the Regulatory 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 revisions to 17 CFR § 240.17a-4 (the "Rule" or "SEC Rule 17a-4"). These revisions to paragraph (f) expressly allowed books and records[1] to be retained on electronic storage media, subject to explicit conditions.

> *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). This Assessment Report includes a summary of the Rule and these two Interpretive Releases in Section 4, *Overview of Relevant SEC Rule 17a-4(f) Electronic Storage Requirements*.

[1] Regulators use the phrase "*books and records*" to describe all content that must be retained under the Rules. Since this assessment deals with the capabilities of a storage solution relative to SEC Rules, Cohasset has chosen to use the term "record object" (versus "data" or "file") to be consistent with SEC terminology.

Additionally, the 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.

In 17 CFR § 1.31 ("CFTC Rule 1.31"), the CFTC defines rigorous requirements for organizations electing to retain books and records on electronic storage media. The June 28, 1999 revisions were the first to authorize books and records to be retained on electronic storage media, subject to explicit conditions. This Assessment Report includes a summary of these requirements in Section 4.2, *Overview of CFTC Rule 1.31(b)-(c) Electronic Storage Requirements*.

Additionally, for the comparable requirements of SEC Rule 17a-4(f) and CFTC Rule 1.31(b)-(c), see Section 4.3, *Comparison of Relevant Requirements of SEC and CFTC Rules*.

1.2 Purpose and Approach

To obtain an independent and objective assessment of the capabilities of ECS features, in comparison to the requirements set forth in SEC Rule 17a-4(f) and CFTC Rule 1.31(b)-(c), Dell EMC engaged Cohasset Associates, Inc. ("Cohasset"). Cohasset is a highly respected consulting firm with more than 40 years of experience and knowledge related to 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 ECS, in comparison to the five requirements related to the recording, storage and retention of electronic records, as stipulated in SEC Rule 17a-4(f) and CFTC Rule 1.31(b)-(c), and
- Prepare this Assessment Report enumerating the results of its assessment.

This assessment represents the professional opinion of Cohasset and should not be construed as either an endorsement or a rejection by Cohasset of ECS and its capabilities or other Dell EMC products or services. The information utilized by Cohasset to conduct this assessment consisted of: (a) oral discussions, (b) user and system administration documentation, and (c) other directly-related materials provided by Dell EMC or obtained from publicly available resources.

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 solutions, meet all seventeen requirements of the Rule.

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 ECS Overview

ECS is a cloud-based object storage appliance that can be configured to utilize integrated control codes to protect stored record objects against deletion or modification. The architecture of ECS is based on the division of storage into multiple Namespaces, with each Namespace being further divided into one or more Buckets where record objects are stored. A Namespace can be configured to enable Compliance, which places additional restrictions on the actions that can be performed on a Namespace and its associated Buckets and record objects, in order to prevent against erasure or overwrite prior to the expiration of an assigned retention period. The additional restrictions, when Compliance is enabled, are designed to meet more stringent regulatory requirements, such as those found in SEC Rule 17a-4(f).

Effective with ECS version 3.0, as of September 2016, ECS is available in two configurations: (1) a fully integrated storage appliance consisting exclusively of Dell EMC branded and tested storage software and hardware, and (2) Dell EMC and ECS Object Storage integrally connected with Dell EMC-certified industry standard hardware.

Accordingly, Cohasset's assessment addresses the ECS Namespace configured to enable Compliance, and also evaluates the use of ECS with Dell EMC-certified third party storage devices. Additionally, this assessment incorporates a general assessment of the Content Addressable Storage (CAS) API interface, including the event-based retention and legal hold capabilities provided by the CAS interface when storing record objects in ECS; and an assessment of the Amazon Simple Storage Service (S3) interface that can be used to store and retain record objects that are compliant with the SEC requirements.

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

This section presents Cohasset's assessment of the capabilities of ECS for compliance with the five (5) requirements related to recording, storage and retention of electronic records, as stipulated in SEC Rule 17a-4(f). See Section 4.3, Comparison of Relevant Requirements of SEC and CFTC Rules.

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

- ***Compliance Requirement*** – A brief explanation, prepared by Cohasset, of the purpose of the specific requirement of SEC Rule 17a-4(f)
- ***Compliance Assessment*** – Assessment of ECS capabilities in relation to its ability to meet the specific requirements of the SEC Rule 17a-4(f)
- ***ECS Capabilities*** – Description of the ECS capabilities that are relevant to the specific requirements of the SEC Rule 17a-4(f)
- ***Additional Considerations*** – Identification of additional considerations for meeting the specific requirements of the SEC Rule 17a-4(f)

The following subsections document Cohasset's assessment of the capabilities of ECS 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."*

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

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

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

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 hold order:

> *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

When the ECS solution is properly configured with Namespaces enabled as Compliant; when Buckets within a Namespace are configured with retention periods appropriate for the record objects being stored and when the considerations identified in Section 2.1.4 are satisfied, it is Cohasset's opinion that the capabilities of ECS meet the requirements of the Rule for (a) managing records as non-rewritable and non-erasable for the assigned retention period(s), (b) directly managing *time-based*[2] retention periods, and (c) allowing retention periods to be extended to address *conditional*[3] retention requirements and preservation for legal holds, as explained in Section 2.1.4.

2.1.3 ECS Capabilities

In this section, the capabilities of an ECS Compliant Namespace that directly affect meeting the requirements of SEC Rule 17a-4(f) for preserving broker-dealer electronic records[4] ("record objects") as non-rewritable and non-erasable, are presented.

Overview

- ECS is a storage appliance where the storage control software and the physical magnetic disk media are combined in an integrated system with no access to the storage media other than through ECS.

[2] Time-based retention periods use the creation or storage date to calculate the retention expiration date.

[3] Conditional or event-based retention periods have an indefinite retention time until a specified event has occurred, then a fixed retention period, calculated from the date stored or event-trigger date to calculate a final retention expiration date.

[4] The term "record" or "record object," rather than just "object," is used in this document to reflect the fact that business transactions, customer information, broker-dealer personnel and certain other administrative files are deemed business records that are required to be maintained for a specific period of time (the retention period) as stated in SEC Rules 17a-3 and 17a-4.

- ECS stores record objects, which encompass the record content and associated system and custom metadata, in a hierarchical structure made up of Namespaces (enabled as Compliant) and associated Buckets.
- Record objects are protected against erasure or overwrite for a specified retention period. One or more retention periods can be assigned to a record object using one or a combination of: (a) a Bucket-level retention period that applies to all record objects stored in the Bucket, (b) Namespace retention policy(ies) assigned to record objects, and/or (c) a specific retention period assigned to a record object.
- A record object cannot be deleted through any mechanism (client/user application or ECS administration) until the longest of the assigned retention periods expires.

Namespace

- The top level of the ECS storage architecture consists of one or more Namespaces.
- For a Namespace to comply with the Rule, it must be configured to enable Compliance. When a Namespace is enabled as Compliant, additional restrictions are enforced in conjunction with integrated control codes that are designed to protect record objects against deletion or modification for the specified retention period.
- Compliance, once enabled for a Namespace, cannot be disabled.
- A Compliant Namespace cannot be deleted if a Bucket within the Namespace contains record objects currently protected by a retention period.
- One or more retention policies can be defined for a Namespace, each with a specific retention period and a unique name or tag. At the time of writing a record object to ECS, the client/user application can assign one or more retention policies which will be stored in the metadata of the record object (once the record object has been recorded, no additional retention policies can be assigned). Once assigned to a record object, the retention policy name is stored in the metadata of the record object and the retention period of the retention policy will be checked when ECS evaluates a deletion request for the record object.
- The retention period defined in a retention policy can be changed to a longer duration, but it cannot be shortened.
- A retention policy that is currently assigned to one or more active record objects cannot be deleted.
- A Namespace may only be configured by users assigned to the Namespace Admin and System Admin roles.
- ECS users are created and assigned to specific Namespaces. Only users assigned to a Namespace may access the record objects belonging to that Namespace.

Bucket

- One or more Buckets **must** be defined for a Namespace.
- A retention period **must** be defined for a Bucket at the time the Bucket is configured. Only one retention period can be defined for a Bucket, and the retention period cannot be zero. This guarantees that the record objects are protected by a Bucket-level retention period.
- The retention period defined for a Bucket can be changed to a longer duration, but cannot be shortened.
  - A retention period can be defined as infinite or updated to be infinite (defined by a -1 code). Once an infinite retention period is assigned, the Bucket and the record objects stored in it can never be deleted.
- Record objects sent to ECS by a client/user application (via an API) must specify the Namespace and Bucket to which they will be recorded. This assures that the appropriate Bucket-level retention period is assigned to the record object.
- A Bucket that contains a record object currently protected by a retention period may not be deleted.

Record Object

- ECS defines a record object as encompassing the content of the object, as well as all associated system metadata and custom metadata. A retention period assigned to a record object also applies to, and protects, the associated system and custom metadata.
  - System metadata includes critical attributes for record object management, such as storage date and time stamp, retention period (in seconds) and the checksum.
  - Custom metadata is optional and can be defined by the broker-dealer for purposes of further identification or retrieval. Custom metadata has no bearing on the retention of record objects.
- A record object is protected against deletion by assigning one or more retention periods. The types of retention periods that can be assigned are described below – multiple retention periods, with limitations noted below, can be assigned to a record object.
  - *First,* the record object is automatically protected by the Bucket retention period where it is stored.
    - The Bucket retention period cannot be zero which assures that all record objects are protected by a retention period. The Bucket retention period can be extended but cannot be shortened.
    - The Bucket retention period applies to all record objects stored in the Bucket. The Bucket retention period is not stored as metadata for each record object. Rather, it is checked when a delete request is received from the client/user application for a record object.
    - If no retention policy and no specific retention period are assigned to the record object by the client/user application, the retention period defined for the Bucket where it is stored is the only retention period that applies to the record object.
  - *Second,* one or more Namespace retention policies (as described in the preceding subsection, entitled "Namespace") may be assigned to a record object by the client/user application when

sending the record object to ECS (once the record object has been recorded, no additional retention policies can be assigned until all retention periods associated with the record object have expired).

        - The name of each assigned retention policy is stored as record object metadata.
        - The retention period in a retention policy can be extended, but not shortened.
        - When a delete request is received for a record object, the retention periods of the assigned retention policies are checked.

    - *Third,* a specific retention period may be assigned to a record object by the client/user application at the time the record object is recorded by ECS.
        - Only one specific retention period can be stored for a record object and it must be assigned at the time of recording. Any assigned retention period is stored as metadata for the record object. If no specific retention period is assigned at the time of recording, then the Bucket level retention period and a retention policy, if assigned at the time of recording, determine the retention time for the record object.
        - The specific retention period cannot be modified, i.e., it cannot be extended, shortened or removed from the record object.
        - After all retention periods that pertain to the record object have expired, a new specific retention period may be assigned and stored as metadata with the record object.
    - Note: There is no requirement that a retention policy or a specific retention period be assigned to a record object, since the mandatory retention period for the Bucket where the record object is stored, automatically protects the record object against deletion until the Bucket-level retention period expires.

- Deletion of a record object is only allowed upon expiration of the longest retention period that is assigned to the record object, i.e., the longest of: (a) the retention period of the Bucket where the record object is stored, (b) the retention period(s) of the retention policy(ies) assigned with the record object (if any), and (c) the specific retention period assigned directly to the object (if any).
    - When a request is made to delete a record object, ECS checks all retention periods assigned to the record object and adds the longest retention period value to the storage date and time of the record object. If the longest retention period has expired, then the record object can be deleted. Otherwise, the delete request is rejected.

Additional Deletion Controls

- Privileged write, which could overwrite an existing record object, is not allowed for a Compliant Namespace. By disallowing this feature, the client/user application and ECS administrator cannot overwrite a record object in a Compliant Namespace prior to the expiration of its assigned retention period.
- Deletion of a record object can only be performed in an ECS Compliant Namespace through an audited delete API command.

  - An audited delete disposes of the specified record object (if its longest retention period assigned to the record object has expired) and creates an audit entry to document that the deletion was performed. An audited delete is performed by an API call and can only be used on record objects after expiration of the longest assigned retention period.
  - Record objects and associated metadata stored in a Compliant Namespace cannot be deleted through any mechanism, by the client/user application or by an ECS administrator, prior to the expiration of the longest assigned retention period.

- Root or system administrator permission does not provide visibility of or access to individual record object location, content or metadata. Therefore, an authorized ECS system administrator or user system administrator does not have the ability to locate and delete or modify individual record objects or any range of record objects. Root level or administrative functions are used for managing ECS at the system configuration or storage system level, such as addressing system errors or storage malfunctions that would require rebooting or performing system or storage-level maintenance activities.

Amazon Simple Storage Service (S3) Interface

The Amazon S3 interface can be used to store, retrieve and retain record objects with ECS.

Extensions have been developed by Dell EMC that allow the S3 interface to:

- Set a policy for a Namespace with a retention period that can be applied to an object by using the policy name when storing a record object in ECS;
- Set and extend a retention period for a Bucket which will then be used as one of the means for determining the retention period for all record objects stored by S3 in the Bucket; and
- Set a retention period for each record object sent to ECS.

When an attempt is made to modify or delete a record object, the longer of the Bucket retention period and a retention period associated directly with a record object – set using the appropriate Namespace retention policy or set directly when stored – is used to determine if the retention period has expired.

It is Cohasset's opinion that the combination of these extensions and controls for the S3 interface meets this requirement of the Rule by ensuring that, when storing record objects in ECS using the S3 interface, the retention protection controls ECS will be employed.

Content Addressable Storage Interface

The Content Addressable Storage (CAS) application interface can be utilized to store record objects in ECS. CAS is the application interface utilized by the Dell EMC Centera product (see Cohasset Associates' Assessment of the Dell EMC Centera Compliance Edition Plus [CE+], dated January 2007). There are unique setup processes in ECS for defining Namespaces and Buckets for use by CAS applications and also a unique setup screen that allows for defining a Bucket retention period, minimum and maximum retention periods and minimum and maximum variable retention periods (for event-based retention). Retention policies (which equate to "retention classes" in CAS) can be defined for a Namespace in ECS and communicated in the C-Clip to apply retention to a record object. Retention periods using the CAS interface can be communicated to ECS in two ways: (1) retention can be set directly at an individual object level using a C-Clip, which is a string of data that contains a unique identifier for the record object plus selected control metadata (such as a retention policy or period), or (2) a Bucket (with a retention period) or a retention policy can be communicated with a record object indicating the Bucket retention period or retention policy that will be applied. In order to be compliant with the Rule, “Enforce Retention Information in Object” must be enabled for a Bucket. All ECS protections are applied to record objects stored using the CAS interface. Accordingly, no deletion is allowed, under any circumstances, until the retention period has expired and all legal holds have been released (see “Time vs. Conditional (Event-Based) Object Retention” below for specific information about event-based retention using the CAS interface).

Time vs Conditional (Event-Based) Object Retention

- Retention management of *time-based* record objects can be achieved by utilizing one or more of the three retention period settings and control capabilities delineated in the preceding subsections entitled “Namespace”, “Bucket” and "Record Object."
- Conditional or event-based[5] retention is available only for those applications that utilize the Content Addressable Storage (CAS) interface to store record objects in ECS.
- To store event-based record objects using CAS, the application must send a C-Clip that is marked as containing an event-based retention policy or retention period (with a minimum retention time period). Once the event has occurred the application sends a C-Clip that indicates the event has occurred and contains a “final” fixed retention period. A CAS record object cannot be deleted until the event has been triggered and the final, fixed retention period has expired (and all legal holds have been released).
- Other, non-CAS, application interfaces that can store record objects in ECS, e.g., S3, Atmos and SWIFT, as well as the ECS Portal and ECS REST APIs, do not currently provide any *inherent* capabilities for managing the event-based retention of record objects.
  - To provide the equivalent of event-based retention in non-CAS environments, ECS provides capabilities that: (a) extend the retention period for an object (potentially multiple times), (b) extend the retention period of applicable retention policies, or (c) extend the Bucket-level retention periods for the objects that are subject to event-based retention. (See the methods described below in section 2.1.4, Additional Considerations). For record objects that require event-based record retention, it is imperative that the appropriate retention period(s) assigned to each record object be extended, multiple times if necessary, to meet the required, full period of retention (the initial indefinite period and the final, fixed retention period, once the event has occurred).

[5] For record objects that require *conditional (event-based)* retention, the retention period must be extended (possibly multiple times) through the indefinite period until the condition is met, i.e., until the triggering event occurs. It must then be extended one last time to retain the record object for the final retention period. For example, to implement the conditional retention period of "Account Closure + 6 Years," the retention period must be extended until the account is closed (the condition is met), and then extended one more time to cover the “final” or “fixed” retention period (e.g., the "6-Year" period) that follows the account closure.

Legal Hold

- When litigation or a subpoena requires record objects to be placed on hold, which could entail retaining them beyond the retention period, the regulated entity must ensure the subject record objects are protected for the duration of the legal hold. There are two means to meet the legal hold retention requirements in ECS:

  1. For applications that use the CAS interface to store record objects in ECS, CAS provides API calls that are supported by ECS to place a legal hold on a record object and to release a legal hold. Multiple holds can be placed on each record object when it is relevant to multiple legal or regulatory actions (multiple C-Clips are utilized to communicate unique hold IDs for each legal hold). A record placed on legal hold cannot be deleted by the controlling application (or by any other means) until all of the retention periods and legal holds associated with a record object have been released, even when the retention period associated with the record object has expired.

  2. For other applications storing records in ECS, a legal hold retention time could be achieved by: (a) extending the retention period of applicable record objects, (b) extending the retention period of the Bucket where the record object is stored, or (c) extending the period for one of the Namespace retention policies assigned to the subject record objects. The process of extending the retention period may need to be performed multiple times, depending on the duration of the legal hold. (See additional details in 2.1.4, Additional Considerations, for the methods that can be used to extend retention periods).

2.1.4 Additional Considerations

The following additional considerations for configuration and usage of a Compliant Namespace are provided to help ensure that the non-erasable, non-rewriteable requirements of the Rule are met for the full time period that the record objects are required to be retained. Specifically, the broker-dealer is responsible for:

- Ensuring each Namespace for storing regulated record objects is configured with Compliance enabled.
- Establishing appropriate Bucket-level retention periods and, where suitable, assigning required retention periods to individual record objects using appropriate retention policies or object-level retention periods.
- Monitoring and extending the retention periods of record objects subject to a conditional (event-based) retention period or a legal hold by using one of the three ECS retention extension methods described below.
  - *First*, the retention period may be extended for the Bucket where the record object is stored.
    - Since the Bucket-level retention period is added to the storage date and time of each associated record object, the extended Bucket-level retention period must consider (a) the date and time the record objects were stored, (b) the estimated duration of the conditional retention period (time until the triggering event occurs, plus the final fixed retention period) and (c) the anticipated duration of the associated legal hold.

  - Further, the extended Bucket-level retention period will apply to all record objects housed in the Bucket. Thus, the above calculation must consider all record objects stored in the Bucket, particularly the most recent or last record object stored.

- *Second*, the retention period for one of the existing Namespace retention policies may be extended.
  - Any extension of the retention period for a Namespace retention policy must be based on a combination of (a) the date and time the record objects were stored, (b) the estimated duration of the conditional retention period (time until the triggering event occurs, plus the final fixed retention period) and (c) the duration of any associated legal hold.
  - Further, the extended retention period will apply to all record objects assigned to the Namespace retention policy.
- *Third*, the specific retention period assigned to the record object may be modified, *<u>after all retention periods assigned to the record object have expired</u>*.
  - Accordingly, the specific record object retention period may be changed to a longer duration *<u>after expiration of:</u>* (a) the associated Bucket-level retention period, (b) the retention period(s) of any assigned Namespace retention policy(ies), *<u>and</u>* (c) the specific retention period assigned directly to the object (if any).
  - This extended retention period applies to only the associated record object.

If the appropriate retention period(s) assigned to the record object are <u>not</u> extended, as required to address the full event-based retention period, the record object is <u>not</u> protected from deletion, once the initially assigned retention period(s) expire.

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 so that 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 ECS capabilities, in conjunction with the inherent capabilities of advanced magnetic storage technology, meet the requirements of the Rule. Specifically, ECS supports or provides for verifying the quality and accuracy of the recording process: (a) during the initial recording of the object record, (b) using post-recording verification during read-back, and, (c) conducting periodic consistency and integrity checking.

2.2.3 ECS Capabilities

ECS 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.
- When a record object is stored in a Compliant Namespace, the client/user application may calculate and send a checksum with the record object. ECS then recalculates the checksum and compares it to the one received from the client/user application. If the checksums are not equal, ECS does not store the record object and returns an error condition to the client/user application.
- During the recording process, ECS uses protect write, wherein three copies of the record object content and metadata are written in parallel in chunks. After the three copies are successfully recorded, ECS writes to the index with name and location and sends an acknowledgement to the client.
- All record objects, metadata and index data are recorded in "chunks". A chunk is a 128MB logical container of contiguous space. Each chunk may have data from different record objects. ECS uses indices to track the parts of an object spread across different chunks. Chunks are written in an append-only manner to avoid overwrite.
    - ECS calculates and stores a checksum for each chunk, which is subsequently used in the post-recording verification processes.
    - Further, for enhanced data protection and recovery, chunks are recorded using the Reed Solomon 12/4 erasure-coding scheme. Each chunk is broken into 12 data fragments and 4 coding fragments; these 16 fragments are dispersed across available storage nodes at the local site. The storage engine can reconstruct a chunk from any 12 of the 16 fragments. Additionally, when creating a new storage pool for cold storage, a 10/2 erasure-coding scheme may be enabled to further reduce storage overhead.

Post-Recording Verification

- During read back of the record object, magnetic disk error detection and correction are applied to correct any in-error data on the magnetic disk. Should the magnetic disk error detection and correction fail to correct the data, then the ECS Reed Solomon 12/4 erasure-coding scheme attempts to correct the error. If unsuccessful, the data is reconstructed from the replicated copy.
- ECS periodically validates the accuracy of all chunks by recalculating each chunk's checksum, and comparing it to the checksum originally calculated and stored with the chunk. If the checksums do not match, the Reed-Solomon 12/4 correction codes are utilized to attempt to correct the in-error chunk. If correction is not successful, the chunk will be reconstructed from the replicated copy.

  - Since ECS writes all data to chunks, the indices, all record objects and associated system and custom metadata are verified through this automated verification process.

- When ECS receives an object retrieval request, the checksum of each associated chunk that the record object is dispersed amongst, is recalculated and verified. It is corrected or recovered from a duplicate copy, if in error.

- At the time the client/user application requests the retrieval of a record object, the client/user application has the option to request a checksum be transmitted with the record object so that it can compare it against the checksum it calculated and sent to ECS with the original storage request.

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."*

While this requirement is thought to be more pertinent to tracking the individual units of removable media related to micrographic or optical storage, the SEC Rule may be satisfied by capturing index data or metadata associated with each electronic record that: (a) *uniquely* identifies the record and (b) associates the *date and time of recording* with each record.

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.

2.3.2 Compliance Assessment

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

2.3.3 ECS Capabilities

ECS utilizes the combination of a unique record object identifier and the date and time the record object was stored, to serialize the record object in both space and time.

- ECS assures each record object within a Bucket has a unique filename.
  - If a record object is sent to ECS using the content addressable storage API, ECS composes its own unique identifier for the record object. The unique identifier is comprised of a hash digest of the record object content, Namespace and Bucket names, within which the record object is stored, and

the date and time of recording. The unique identifier is sent back to the client/user application for storage in its directory so the record object can be requested back from ECS using the unique identifier.

- ◆ When a record object is submitted to ECS with a predefined filename, ECS adds the Namespace and Bucket name to the filename provided by the client application. The new filename is stored in ECS, along with the date and time of recording, as system metadata of the record object.

- The date and time each record object is stored to ECS is recorded as part of the system metadata and protected from alteration for the longest retention period associated with the record object.

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 for downloading records and indexes to an acceptable medium is designed to enable the SEC to request a broker-dealer to download the records and associated indexes from the primary storage medium, to a medium acceptable under the Rule, e.g., micrographics or electronic storage media. 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 ECS meet the requirements of the Rule by providing the capabilities for an administrator or client\user application to request a Bucket list or to execute a query to create a list of record objects and the associated metadata. Then to select and download all or part of the list and, using local capabilities, reproduce the records or transfer them to a medium acceptable under the Rule.

2.4.3 ECS Capabilities

ECS supports efforts to assure the capacity to download record objects and metadata.

- Using the unique identifier assigned by ECS when the record object is stored, the client/user application can request one or more record objects to be retrieved from ECS. 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 the API calls or queries, a list of selected or all record objects stored in a Bucket, can be requested or searched.

  - ◆ The result of the API call is a list of some or all objects in a Bucket.

- The result of a query is a list of the identifier and/or metadata for record objects matching the query parameters.

Once the Bucket list of record object identifiers/metadata or the query list of record object identifiers/metadata is available, other API commands are used to select and retrieve 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 object(s) to a medium acceptable under the Rule.

2.4.4 Additional Considerations

The broker-dealer 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* is different from a *backup copy*. A *duplicate copy* is recorded at or near the time of the original, allows for the complete record to be reestablished, is stored on a compliant storage system or media, and is retained for the same time period as the originally stored record. A *backup copy*, in contrast, is typically overwritten as it is “rotated” on a periodic basis, which usually results in a much shorter retention period than the original.

2.5.2 Compliance Assessment

It is Cohasset’s opinion that ECS meets this requirement of the Rule by defining replication groups and utilizing geo-replication to ensure that a primary copy of the record object is stored at the original/receiving Virtual Data Center (VDC) and that a replica or duplicate copy is stored at a second VDC – or across multiple VDCs if more than two. When writing to three or more VDCs, Cohasset also believes that the "contraction (XOR)" process utilized by ECS to reduce storage overhead for the replica stored across multiple VDCs meets the requirements of the Rule. When a record object is requested and the original copy is not available, a reverse "expansion" process is employed to completely and accurately reconstruct a duplicate from the sites where the replica is stored to fulfill the request.

2.5.3 ECS Capabilities

In ECS, a replication group must be defined with allocated storage pools where a replicated copy of a record object will be stored. In a configuration with more than two VDCs, the replicated copy may be stored utilizing a "contraction (XOR)" process to reduce storage overhead across the multiple sites. The replicated copy can then can be located and expanded, as a complete duplicate copy, to satisfy a record object request, when the primary record object is not available from the original VDC.

- A replication group is a logical collection of storage pools (locations where record object chunks are recorded) which provide locations for replicating a record object recorded in an original storage pool to one or more additional storage pools at multiple VDCs.
  - When an ECS configuration has only two VDCs, the replication group is configured to store a full replica of the original copy to the second VDC.
  - When an ECS configuration has three or more VDCs:
    - Either:

      (a) The replication group may be configured to enable the storage of a full replica of the original at each of the sites for maximum data protection and enhanced read performance, or

      (b) A contraction/XOR function may be utilized, for purposes of storage efficiency, to replicate record objects from the first site jointly to the second and third (or more) sites. Similarly, a record object written to the second site will be replicated jointly to the first and third (or more) sites. This contraction/XOR process reduces the amount of storage required to store the replica. When a record object is requested by a client/user and the original copy is not available, ECS utilizes an XOR expansion process to reconstruct a complete and accurate duplicate of the original from the replicas jointly stored across the configured VDC sites and provide it to the requester.
    - If the original copy continues to be unavailable, ECS creates another copy so that at least two copies of the record object are available at all times for retrieval.
- The metadata (index) for each record object is stored in triple mirrored chunks for protection and is also cached in memory to aid frequent access. The metadata for each record object also is mirrored to all remote sites in the replication group.

2.5.4 Additional Considerations

The broker-dealer must configure and assign replication groups and necessary storage pools to the Compliant Namespaces and associated Buckets to ensure that a primary and replica copy of each record object is stored and retained. Using geo-replication, each site may store a complete replica, or when ECS is configured with three or more VDCs, the contraction/XOR function may be enabled to store a replica across multiple sites, allowing for complete and accurate reconstruction of the record object. Replication at multiple geographic sites is required.

3 | Conclusions

Cohasset assessed the functionality of ECS in comparison to the recording, storage and retention requirements and conditions of SEC Rule 17a-4(f) and the two associated SEC Interpretive Releases, as well as the relevant storage requirements of the CFTC Rule 1.31(b)-(c). Cohasset determined that ECS has the following capabilities, which support its ability to meet the recording, storage and retention requirements:

- Maintains record objects in a non-erasable and non-rewriteable format for *time-based*[6] retention periods.
- Provides *conditional (event-based)*[7] retention when using the CAS interface to store record objects and, otherwise, allows selected retention periods (stored in seconds) to be extended to address record object preservation requirements for subpoenas or legal holds, as explained in Section 2.1.4. Also provides setting and releasing a legal hold on record objects when utilizing the CAS interface.
- Prohibits deletion of a record object and its metadata until all associated retention periods have expired.
- Automatically verifies the accuracy and quality of the recording process utilizing (a) advanced storage recording technology (such as magnetic storage, and (b) a checksum that is calculated during the recording process and is stored as a metadata attribute and utilized for post-recording verification.
- Uniquely identifies and chronologically serializes each stored record object.
- Provides for an administrator to produce lists, such as a list of all record objects stored in a Bucket or a list of the results of a query, which show the metadata for selected record objects and permits the retrieval or downloading of the record objects and metadata for local reproduction or transfer to a medium acceptable under the Rule.
- Uses replication groups to replicate all record content and integrated control code metadata to a second storage pool to assure that at least two replicas of the record objects and associated metadata are stored.

Cohasset's assessment also finds that the use of industry standard hardware storage devices that are certified by Dell EMC in conjunction with ECS object storage are compliant with the Rule.

Accordingly, Cohasset concludes that ECS version 3.0, when properly configured and managed, meets the five SEC 17a-4(f) and CFTC 1.31(b)-(c) requirements that relate directly to the recording, storage, availability and retention of record objects.

[6] Time-based retention periods use the creation or storage date to calculate the retention expiration date.

[7] Conditional (event-based) retention periods, e.g., Account Closure + 6 Years, require the record object to be retain indefinitely until the triggering event occurs (e.g., the account is closed). When the triggering event occurs, the remaining retention period (e.g., 6 Years) can be assigned. As noted in Section 2.1.4, ECS has limited capabilities to manage conditional or event-based retention periods.

4 | Overview of Relevant SEC and CFTC Requirements

This section establishes the context for the regulatory requirements that are the subject of this assessment by providing an overview of the SEC and CFTC regulatory foundation for allowing electronic records to be retained on a variety of compliant electronic storage media.

4.1 Overview of SEC Rule 17a-4(f) Electronic 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 allowed records to be retained on electronic storage media, subject to meeting certain conditions. Additionally, the Financial Industry Regulatory Authority (FINRA) Rule 4511(c) stipulates:

> *(c) All books and records required to be made pursuant to the FINRA rules shall be preserved in a format and media that complies with SEA Rule 17a-4.*

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 SEC Rule 17a-4, 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, 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).*

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.*

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

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

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

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

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

> *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 <u>storage system must allow records to be retained beyond the retentions periods specified in Commission rules.</u> [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) under the jurisdiction of the SEC, such as the Financial Industry Regulatory Authority (FINRA).

4.2 Overview of CFTC Rule 1.31(b)-(c) Electronic Storage Requirements

Recordkeeping requirements promulgated by Commodity Futures Trading Commission (CFTC) include 17 CFR § 1.31 (CFTC Rule 1.31). When effective on June 28, 1999, CFTC Rule 1.31 authorized entities under the regulatory jurisdiction of the CFTC to retain records on an electronic storage media or system, subject to the requirements and conditions of the Rule. The Commission has modified CFTC Rule 1.31 over time; however, these modifications have not substantively affected the explicit requirements for electronic storage media, which are the basis of this assessment.

However, recent changes to CFTC Rule 1.31(a)-(b), amended in response to The Dodd-Frank Wall Street Reform and Consumer Protection Act and effective January 2, 2013, significantly expanded the requirement for a regulated entity to retain its existing electronic records, which must be kept in *native file format*. CFTC Rule 1.31(b) states:

> *(b) Except as provided in paragraph (d) of this section, books and records required to be kept by the Act or by these regulations may be stored on either "micrographic media" (as defined in paragraph (b)(1)(i) of this section) or "electronic storage media" (as defined in paragraph (b)(1)(ii) of this section) for the required time period under the conditions set forth in this paragraph (b); Provided, however, For electronic records, such storage media must preserve the native file format of the electronic records as required by paragraph (a)(1) of this section. ***** [emphasis added]*

The CFTC Rule 1.31(a)(1) defines *native file format* as:

> ******[N]ative file format means an electronic file that exists in the format in which it was originally created.*

The issue of technology obsolescence and the need to migrate data from its current *native file format* is discussed in the November 2, 2012, Federal Register, which published the amended final rules. Specifically, *II. Comments Received and Amended Regulations*, includes the following excerpts:

> *[T]he Commission is now making clear that paper records are not usable by the Commission as a substitute for the underlying financial data used to create that paper.*
> *Therefore, it is necessary that electronic records be maintained in their native file format and not reduced to paper. Accordingly, for records that include data stored in a database, the ''native file format'' is the format in which the data is maintained in that database, not a format reduced to paper or imaged format, which is essentially the equivalent of paper.*
> *[T]he Commission confirms that maintaining data in native file format (i.e., the format in which it was originally created or maintained) does not prohibit a recordkeeper from migrating that data from an obsolete or legacy system or database to a new system or database, where it will then be maintained in the native file format of the new system or database. [emphasis added]*

Accordingly, the CFTC recognizes that the *native file format* may change over time, due to data migrations, for example.

It is important to emphasize that this requirement to retain electronic records in *native file format* does **not** change the requirements of CFTC Rule 1.31(b)-(c) for electronic storage media of the electronic records.

The electronic storage media requirements of CFTC Rule 1.31(b)-(c) are substantively the same as promulgated in the Federal Register on May 27, 1999. Further, these individual requirements are very similar to, and in some cases essentially identical to, the equivalent electronic storage system requirements that are defined in SEC Rule 17a-4(f), including the requirement to "*Preserve the records exclusively in a non-rewriteable, non-erasable format.*" When issuing the final Rule the Commission stated:

> *In view of the significant number of firms subject to regulation under both the federal commodity and securities laws, the final regulations recognize the value of maintaining consistency, where possible, between the Commission's approach to recordkeeping and that of the SEC. The regulations do not reflect strict conformity with the regulations the SEC adopted in 1997, however, because the Commission concluded that there were significant differences between the commodities and securities industry that justified retaining certain of its current rules.*

To evaluate the applicability of the SEC's Interpretive Releases, including authorized use of erasable and rewritable media, to the recordkeeping requirements of the CFTC, Cohasset reviewed the information published in the May 27, 1999, Federal Register. This Federal Register published the CFTC's adoption of the amendments to CFTC Rule 1.31 and contained the following excerpt in the *Supplementary Information*:

> *On several occasions during the past two years, the Commission has provided interim relief from the current requirements of Rule 1.31 to Commission registrants using advanced technology(44).*

In footnote (44), the Commission states:

> *The Commission has permitted these registrants to substitute compliance with the SEC's recordkeeping requirements for compliance with current requirements of Rule 1.31 ******

This footnote describes the CFTC's willingness to rely, where appropriate, on the SEC's rules and its history of granting permission to alternatively substitute compliance with the SEC's recordkeeping requirements, for compliance with the requirements of CFTC Rule 1.31. This suggests that it is reasonable to conclude that the CFTC would accept compliance with the SEC 2003 Interpretive Release as a substitute for, or a complement to, the Commission's rulemaking related to CFTC Rule 1.31(b)-(c).

In the *Supplementary Information* provided with CFTC Rule 1.31, the CFTC also acknowledges that registrants would benefit from the use of evolving storage media and technology, by stating:

> *The Commission recognizes the important role improved technology can play in the continued development of the futures industry. Minimizing unnecessary regulatory obstacles to the [adoption] of improved technology is a goal of industry members, customers, and the Commission.*

One basic difference between the CFTC Rule and the SEC Rule, is that the CFTC Rule only requires notification to the Commission prior to placing a compliant system into production. The SEC Rule, however, requires the regulated entity to send a notification letter to the appropriate Designated Examining Authority (DEA) ninety (90) days prior to deploying a compliant non-WORM system.

Even though the CFTC has not issued any formal interpretive releases or statements subsequent to the effective date of CFTC Rule 1.31, nor have they indicated direct support of the SEC's 2003 Interpretive Release, it is Cohasset's opinion that the CFTC would interpret the use of advances in digital storage media and systems technology (such as erasable magnetic storage using the integrated control codes stipulated in the 2003 SEC Interpretive Release) as compatible with the vision and intentions of the CFTC for CFTC Rule 1.31(b)-(c).

Also see the following section for a comparison of the storage requirements of the SEC and CFTC Rules.

4.3 Comparison of Relevant Requirements of SEC and CFTC Rules

The individual relevant requirements cited in the body of this report are based on the wording in SEC Rule 17a-4(f). The SEC requirements that are cited in this report are very similar in number, principal and context, if not always in their wording, to requirements stated in CFTC Rule 1.31(b)-(c).

For cross reference, the table below provides a one-for-one comparison of the relevant recording, storage and retention requirements of SEC Rule 17a-4(f) with the similar requirements of CFTC Rule 1.31(b)-(c).

The following requirements reflect the most recent updates to SEC 17a-4(f)(2)(ii)(A)-(D) and CFTC 1.31(b)(1)(ii)(A)-(D).

SEC 17a-4 Requirement		CFTC 1.31 Requirement	
(f)(2)	If electronic storage media is used by a member, broker, or dealer, it shall comply with the following requirements:	(b)	Except as provided in paragraph (d) of this section, books and records required to be kept by the Act or by these regulations may be stored on either “micrographic media” (as defined in paragraph (b)(1)(i) of this section) or “electronic storage media” (as defined in paragraph (b)(1)(ii) of this section) for the required time period under the conditions set forth in this paragraph (b); Provided, however, For electronic records, such storage media must preserve the native file format of the electronic records as required by paragraph (a)(1) of this section.
(f)(2)(ii)	The electronic storage media must:	(b)(1)(ii)	The term “electronic storage media” means any digital storage medium or system that:
(f)(2)(ii)(A)	Preserve the records exclusively in a non-rewriteable, non-erasable format;	(b)(1)(ii)(A)	Preserves the records exclusively in a non-rewritable, non-erasable format;
(f)(2)(ii)(B)	Verify automatically the quality and accuracy of the storage media recording process;	(b)(1)(ii)(B)	Verifies automatically the quality and accuracy of the storage media recording process;
(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; and	(b)(1)(ii)(C)	Serializes the original and, if applicable, duplicate units of storage media and creates a time-date record for the required period of retention for the information placed on such electronic storage media; and
(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.	(b)(1)(ii)(D)	Permits the immediate downloading of indexes and records preserved on the electronic storage media onto paper, microfilm, microfiche or other medium acceptable under this paragraph upon the request of representatives of the Commission or the Department of Justice.

The following requirements reflect the most recent updates to SEC 17a-4(f)(3)(iii) and CFTC 1.31(b)(2)(iv).

SEC 17a-4 Requirement		CFTC 1.31 Requirement	
(f)(3)	If a member, broker, or dealer uses micrographic media or electronic storage media, it shall:	(b)(2)	Persons who use either micrographic media or electronic storage media to maintain records in accordance with this section must:
(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.	(b)(2)(iv)	Store a duplicate of the record, in any medium acceptable under this regulation, at a location separate from the original for the period of time required for maintenance of the original; and

About Cohasset Associates, Inc.

Cohasset Associates, Inc. (www.cohasset.com) is one of the nation’s foremost management consulting firms specializing in records management and information governance. Spanning 40 years and serving both domestic and international clients, Cohasset provides award-winning professional services in four areas: management consulting, education, thought-leadership and legal research.

Management Consulting: Working with multi-national clients, Cohasset develops effective records and information management programs that promote interdisciplinary governance. Cohasset also engages in implementation activities to achieve business goals, improve compliance and mitigate risk. Distinguished as a leader of the transition from records management to information governance, Cohasset held its first Managing Electronic Records (MER) Conference in 1993.

Education: Cohasset is renowned for its longstanding commitment to education on information governance and records and information lifecycle management.

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

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

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 unneeded information*
- *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*

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*. It is this blend of practical experience and a clear vision of the future, which, combined with its commitment to excellence, has resulted in Cohasset's extraordinary record of accomplishments and innovation.