Cohasset Associates

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

Cohesity DataPlatform

Abstract

BENEFIT FROM COHASSET'S INDUSTRY INSIGHT AND EXPERIENCE

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

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

Cohesity DataPlatform enables organizations to consolidate secondary data, objects and associated management functions onto one unified platform, either on-premises or in the public cloud. The Cohesity *DataLock* feature is designed to meet securities industry requirements for preserving records in a non-rewriteable and non-erasable format. When the *DataLock* feature is utilized on Cohesity DataPlatform, stringent retention and immutability controls protect regulated records.

In this Assessment Report, Cohasset Associates, Inc. ("Cohasset") assesses the capabilities of Cohesity DataPlatform relative to the electronic records recording, storage and retention requirements of the:

- Securities and Exchange Commission (SEC) in 17 CFR § 240.17a-4(f), which regulates exchange members, brokers or dealers.
- Financial Industry Regulatory Authority (FINRA) Rule 4511(c), 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 Cohesity DataPlatform version 6.0, when properly configured and utilized with the *DataLock* feature to store and retain *time-based* records in a non-erasable and non-rewriteable format, 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 Cohasset's detailed assessment of SEC requirements, Section 3 for a summary assessment of CFTC requirements, Section 4 for conclusions, and Section 5 for an overview of the relevant Rules.

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.

Cohesity DataPlatform, utilized with the DataLock feature, is designed to support compliance with the stringent requirements for the recording, storage and retention of regulated books and records. To evaluate its compliance capabilities with SEC and CFTC requirements, Cohesity engaged Cohasset to complete an independent and objective assessment of Cohesity DataPlatform, utilized with the DataLock feature, relative to these requirements.

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

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 "SEC Rule"). 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 chosen to use the term "record object" (versus "data," "file" or "object") to consistently recognize that the content is a required record.

1.1.2 FINRA Rule 4511(c) Requirements

Financial Industry Regulatory Authority (FINRA) Rule 4511(c) 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* s in 17 CFR § 1.31(a) is essential to the CFTC's electronic recordkeeping requirements.

> *Regulatory records means all books and records required to be kept by the Act or Commission regulations in this chapter, including any record of any correction or other amendment to such books and records, provided that, with respect to such books and records stored electronically, regulatory records shall also include:*
>
> *(i) Any data necessary to access, search, or display any such books and records; and*
>
> *(ii) All data produced and stored electronically describing how and when such books and records were created, formatted, or modified.* [emphasis added]

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

Refer to Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*, which relates the CFTC principles-based requirements to the capabilities of Cohesity DataPlatform, 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 Cohesity DataPlatform version 6, utilized with the *DataLock* feature, in comparison to relevant storage-specific requirements set forth in SEC Rule 17a-4(f) and CFTC Rule 1.31(c)-(d), Cohesity 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 Cohesity DataPlatform version 6, utilized with the *DataLock* feature, in comparison to the five requirements related to recording, storage and retention of electronic records, as stipulated in SEC Rule 17a-4(f); 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 Cohesity DataPlatform; 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 Cohesity DataPlatform and its capabilities or other Cohesity 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 Cohesity 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 Cohesity DataPlatform Overview

Cohesity DataPlatform is designed to consolidate secondary data, objects and associated management functions onto one unified solution. Cohesity DataPlatform can be deployed on physical or virtual appliances, in a regulated entity's information systems environment, or on virtual appliances in the public cloud.

The *DataLock* feature is designed specifically to store record objects in Cohesity DataPlatform, in compliance with SEC Rule 17a-4(f). Record objects, comprised of files/objects and associated system metadata, are retained in datastores, called Views. When the *DataLock* feature is applied, at either the File (record object) level or the View level, a *Lock Until* (retention expiration) date is assigned and stringent retention and immutability controls are applied to protect the record objects in a non-rewriteable and non-erasable format for the duration of the assigned retention period. Additionally, once the retention period has passed, record objects with the *DataLock* feature applied at the File-level will continue to be protected against modification or overwrite until deleted from the Cohesity system.

Throughout this Assessment Report, Cohasset's use of Cohesity or Cohesity DataPlatform refers to Cohesity DataPlatform version 6 solution, properly configured and utilized with the *DataLock* feature.

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

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

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

- ***Compliance Requirement*** – Excerpt of each electronic storage requirement in SEC Rule 17a-4(f) and Cohasset's interpretation of the requirement.
- ***Compliance Assessment*** – Assessment of the relevant capabilities of Cohesity DataPlatform
- ***Cohesity DataPlatform Capabilities*** – Description of relevant capabilities of Cohesity DataPlatform
- ***Additional Considerations*** –Additional considerations related to meeting the specific requirement

The following subsections document Cohasset's assessment of the capabilities of Cohesity DataPlatform relative to each pertinent requirement of SEC Rule 17a-4(f).

2.1 Non-Rewriteable, Non-Erasable Record Format

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

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

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

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

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

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

> *Moreover, there may be circumstances (such as receipt of a subpoena) where a broker-dealer is required to maintain records beyond the retention periods specified in Rule 17a-4 or other applicable Commission rules. Accordingly, a broker-dealer must take appropriate steps to ensure that records are not deleted during periods when the regulatory retention period has lapsed but other legal requirements mandate that the records continue to be maintained, and the*

> *broker-dealer's storage system must allow records to be retained beyond the retentions periods specified in Commission rules.* [emphasis added]

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

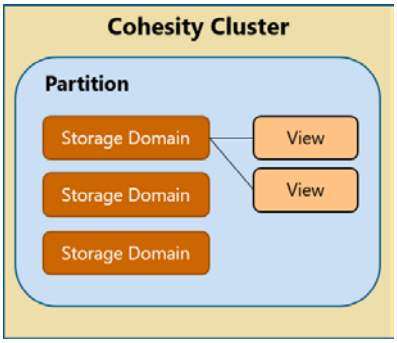
2.1.2 Compliance Assessment

It is Cohasset's opinion that the current capabilities of Cohesity DataPlatform meet this requirement of the SEC Rule to retain *time-based*[3] record objects in non-erasable and non-rewriteable format when (a) Cohesity DataPlatform is properly configured and managed, (b) the *DataLock* feature is enabled at either the View or File (record object) level, (c) an appropriate retention expiration date is assigned as the *Lock Until date*, and (d) the additional considerations in Section 2.1.4 are satisfied.

2.1.3 Cohesity DataPlatform Capabilities

In this section, Cohasset presents the current capabilities of Cohesity DataPlatform, utilized with the *DataLock* feature, that directly pertain to the SEC Rule 17a-4(f) requirement for preserving electronic records as non-rewritable and non-erasable, for the required retention period.

General



- Cohesity DataPlatform architecture, at the highest level, is comprised of a Cohesity Cluster. A Cluster is a collection of physical storage nodes which are assigned to a logical partition. The partition contains one or more Storage Domains (named storage locations), which are further sub-divided into datastores, referred to as Views. A View is used to store files, objects, directories and system metadata. Record objects can be transferred and stored in a View using the NFS, SMB and S3 interfaces.
- Cohesity DataPlatform defines and manages *record* information at the individual record object level, which is comprised of:
  - Complete content of the record object.
  - Immutable record object metadata, e.g. a 64-bit ID (unique to every file), data location (node, disk, offset), checksum, file name and creation (storage) date and time.
  - Mutable record object metadata, e.g. *Lock Until Date* (retention expiration date) for record objects controlled at the File level by the *DataLock* feature. Note: The *Lock Until Date* may only be extended, not shortened or deleted.

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

- Cohesity DataPlatform manages *retention* via the *DataLock* feature, at either the File (record object) or View level. When the *DataLock* feature is applied, stringent retention protection and management controls are applied. See the Retention section, below, for more details.
  - ***File-level:*** The *DataLock* feature is enabled, and retention rules defined, during the initial *Create View* process prior to record objects being stored within the View.
    - Once *File DataLock* is enabled, a *Lock Until* (retention expiration) date is assigned to each record object based upon a triggering attribute, either (a) immediately, as it is written to the View, or (b) after a specified period of inactivity. The *Lock Until* date that is assigned can be transmitted from the source system or calculated by the Cohesity system, based on the View's default retention rules.
  - ***View-level:*** The *DataLock* feature is enabled as part of the *Clone View* process, for Views that already retain record objects. Enabling this feature creates a duplicate of the original View (hereinafter *DataLock View*) and all its existing contents. Once enabled at the View-level:
    - A single *Lock Until (*retention expiration) date is defined for the *DataLock View* and used to govern retention of all record objects contained within that *DataLock View*.
    - *DataLock View* System metadata includes:
      - Immutable attributes such as a 64-bit ID (unique to each *DataLock View*), data location (node, disk, offset), and checksum.
      - Mutable attributes such as the Lock Until date (Note: The *Lock Until* date may only be extended, not shortened or deleted) and optional, user-defined attributes for purposes of further identification.
- Record objects and associated system metadata, protected by the integrated control codes of the *DataLock* feature, cannot be deleted through any mechanism prior to the associated *Lock Until* date. Further, *DataLock* prohibits:
  - Overwriting or modifying the fixed content of a successfully stored record object;
  - Overwriting or renaming a View;
  - Shortening or deleting the retention period assigned to a record object or *DataLock View*; and
  - Appending additional record objects to a *DataLock View*.

Retention and Immutability Controls

- ***File-level DataLock:***
  - File (record object) level retention and immutability controls are defined for a View intended to store compliant record objects, by applying the *File DataLock* feature during the *Create View* process. This can be accomplished by authorized users via user interface, or automatically, via API's.
  - The following settings are available during the *Create View* process to define how retention and immutability controls are to be assigned to record objects during the recording process.

- A Default Retention duration (e.g. seconds, minutes, hours, days, months or forever) from the record object's creation (storage) date/time must be defined. This value will be used to compute a record object's retention expiration date in certain circumstances, such as when a specific retention expiration date is not provided by the source system.
- Minimum and Maximum Retention (optional). The Minimum and/or Maximum retention values (I.e. the number of months or years a record object is retained past its creation date/time) are used to validate that retention expiration dates supplied by the source system are within an allowable range.
- Immutability and retention controls are applied to a record object via the following:

  1. ***Manual Lock*** is a required setting which specifies whether the Read-Only (file permission) attribute or FutureATime (i.e., access time or atime) attribute will trigger the application of the controls. When a record object is stored, it remains **unprotected** until the designated trigger is provided, at which time retention and immutability controls are applied.
     - *Read-Only Trigger:* When the Read-Only attribute is set, the record object is locked and the Default Retention value is applied as the *Lock Until* date.
       - Optionally, a future atime may be provided. If it is valid (within the min/max range), the supplied atime is used as the *Lock Until* date, otherwise the Default Retention value is used.
     - *FutureATime Trigger:* When a *valid* (within the min/max range) future atime is provided, the record object is locked and the atime is applied as the *Lock Until* date. If the provided atime is *invalid*, the Lock Until date will *not* be assigned, an error is issued, and the source system must correct.
  2. ***Autolock Files*** is an optional feature that can be used as a supplement to *Manual Lock*. When enabled, *Autolock Files* automatically locks record objects and applies immutability controls after a designated period of inactivity.
     - The inactivity period for Autolock is defined by the regulated entity as the duration of time that must have elapsed (e.g. seconds, minutes, hours) from the *last modified* time stamp. Ideally, all regulated records should be locked within 24 hours of being written to the View.
     - The *Lock Until* date applied to the record object is derived from the Manual Lock process described above. The exception is that if FutureATime is the trigger and no future atime value is provided, the record object will be locked, using the Default Retention value as the *Lock Until* date.
     - Note: Autolock settings are ignored in cases where the Read-Only attribute is (a) the designated trigger for a View, and (b) a record object is transmitted with this attribute set. The record object will be locked immediately when written to the View and will not be subject to the Autolock Files waiting period.

- System users assigned to the Data Security Role can modify the following *File DataLock* settings for a View:
  - Default Retention can be increased, but never reduced.
  - Autolock File I/O activity duration
  - Manual Lock File options (Read-Only or FutureATime)
  - Minimum and Maximum Retention periods

  Once modified, changes will only apply to new records stored within the View.
- Once set, the *Lock Until* dates assigned to record objects within a View may be
  - Globally extended to a single date in the future, via the Override option on the Edit View screen. Note: if a record object's current *Lock Until* date exceeds the new extended date, the original *Lock Until* date will remain unchanged.
  - Individually extended via Powershell commands or REST APIs.
  - *Lock Until* dates may never be shortened or deleted.
- A record object that is past its retention period will continue to be protected against modification and overwrites until deleted.
- Once *File DataLock* is enabled for a View it cannot be disabled.
- If a View with *File DataLock* enabled is cloned, via Cohesity's *Clone View* process, the *DataLock* control codes associated with the source View are **not** carried over to its clone. Therefore, contents of the clone will not be protected against modification, overwrite or deletion unless separately protected.
- If replication is enabled within Cohesity DataPlatform, *File DataLock* control codes associated with a source View will be carried over to the replicated View, including any extensions made to *Lock Until* dates. Refer to section 2.5 for additional information regarding replication.

▶ ***View-Level DataLock:***

- A single retention date and immutability controls may be established and managed at the View level by enabling the *DataLock* feature during the *Clone View* process. This process is accomplished manually via user interface, or automatically via REST APIs.
  - *Manual DataLock Process* - When all record objects have been written to the View, the system user assigned to the Security Role:
    - Invokes the *DataLock* process via the Clone as *DataLock View* screen,
    - Identifies the longest retention period associated with a View's records and assigns it as the single *Lock Until* date for the *DataLock View*.
  - *DataLock Process via REST API's* – Alternatively, REST API's may be utilized to:
    - Automate the process of writing records to a View,

        - Invoke the *DataLock* process for the View when it has completed writing records to the View, and
        - Identify and transmit the longest retention period associated with the View's record objects. This date will then be used to set the *Lock Until* date for the *DataLock View*.
    - Once set, the *Lock Until* date for a *DataLock View* may be extended manually via the View Edit screen but cannot be reduced or deleted.
    - Following the execution of the *DataLock* process, two copies of a View exist:
        - *Immutable* - a read-only, immutable copy of the original View, including all record objects and associated system metadata from the original. The *Lock Until* date is added as critical system metadata for the *DataLock View*. This *DataLock View* contains the official records for the regulated entity.
        - *Mutable* – the original View will remain available and may be used for test/development purposes. This View must no longer be used for SEC-regulated records storage. Any new records, or modifications to existing records, should be captured in a new View with *DataLock* enabled.
    - If replication is enabled within Cohesity DataPlatform, control codes from each primary *DataLock View* will not be carried over to the replicated View. Therefore, it will be necessary for the regulated entity to immediately execute the *DataLock* process on each replicated View and supply the same *Lock Until* date as the original. Refer to section 2.5 for additional information regarding replication.
- Once a *DataLock View* is past its retention period, immutability controls are removed, allowing its record objects to be modified, overwritten or deleted from the Cohesity system.
- The capabilities of Cohesity DataPlatform are currently limited to time-based records, i.e. records where a retention period is applied at the time of recording and is effective for a fixed, contiguous period of time. Cohesity DataPlatform supports time-based retention periods by assigning a *Lock Until* date to the record object or *DataLock View*. Records with event-based[4] retention requirements should be retained in a separate compliance system.

Legal Hold

- When a subpoena or legal hold requires record objects to be retained beyond their *Lock Until* date, the *Lock Until* date can be extended by users with the Security role.
    - *Lock Until* dates for record objects managed at the **View-level** are extended by modifying the *Lock Until* field on the View Edit screen.
    - *Lock Until* dates for record objects managed at the **File-level** may be globally extended through the Override option on the View Edit screen. When the Override option is selected and an Override (extension) date is provided:

[4] Event-based or event-time-based retention periods require the record object to be retained indefinitely until a specified event occurs (e.g., a contract expires, or an employee terminates), after which the record object must be retained for a fixed final retention period. Both the SEC and CFTC have defined recordkeeping obligations that require event-based retention periods.

- The *Lock Until* date is extended for every record object in the View whose current *Lock Until* date does not exceed the Override (extension) date. No change is made for those record objects with a *Lock Until* date that exceeds the Override (extension) date. Alternatively, *Lock Until* dates for record objects managed at the File-level may be extended individually via Powershell commands or REST APIs.
- The *Lock Until* date*, for the DataLock View or the record objects,* can continue being extended, repeatedly, if necessary, until the legal hold is released.
- The *Lock Until* dates can never be reduced once set.

- Optionally, the View description field may be modified by authorized users to track the reason for the hold.
- If replication is enabled within Cohesity DataPlatform, the *Lock Until* dates at the File-level or View-level and the View description fields must be applied to the replicated Files or Views affected by a subpoena or legal hold.

Disposition/Deletion

- Regardless if retention is controlled at the File-level or View-level, record objects and associated metadata may only be deleted after the applied *Lock Until* date has expired.
- Once eligibility is confirmed:
  - Users assigned to the Data Security Role are authorized to execute the deletion of a *DataLock* View, including all records contained within it, via the user interface.
  - If retention is controlled at the File-level, bulk deletion of individual record objects is managed by NFS, SMB or S3 interfaces.
- The deletion process must be repeated for all replicated copies of individual record objects or *DataLock* Views which exist.
- Privileged delete is not allowed for a locked record object or *DataLock View*. Accordingly, the administrative deletion of a locked record object or View, prior to expiration of the *Lock Until* date, is prohibited.

Clock Synchronization

- To protect against the possibility of premature deletion of records that could result from accelerating the system time clock, a Network Time Protocol (NTP) server must be specified when a Cohesity Cluster is created.

Security

- In addition to the stringent retention protection and management controls described above, Cohesity DataPlatform provides the following security capabilities to help ensure the authenticity and reliability of record objects.
  - Access Controls – Cohesity DataPlatform utilizes role-based security to define privileges for users within the Cohesity Cluster. A Cluster can be joined to an Active Directory domain, allowing for authentication of both users and SMB interfaces, based on Active Directory credentials.
  - Encryption – Software-based AES-256 encryption, with optional FIPS certification, can be enabled on Cohesity DataPlatform to:

- Encrypt the content of Views at rest on the platform and in flight during replication.
- Automatically decrypt Views for use.
- Automatically rotate and manage encryption keys or utilize an external key management system.

- For record objects that are encrypted by the regulated entity *prior* to uploading to Cohesity DataPlatform:
  - An additional layer of encryption will be applied by Cohesity DataPlatform (if encryption is enabled) to help secure the record objects.
  - The regulated entity is responsible for maintaining its own encryption keys to decrypt the record objects for use.

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:

- Ensuring that the file name and creation (storage) date/time are transmitted with each regulated record object stored within the Cohesity system.
- Assuring that all record objects that are required for regulatory compliance are protected with an appropriate *Lock Until* date, using either the File-level or View-level retention management features.
  - If **File-level** retention management is applied,
    - Transmitting the attributes necessary to trigger the application of immutability and retention controls.
    - Defining allowable Minimum and Maximum retention periods for validating transmitted retention expiration dates.
    - Setting an appropriate Default retention period for use when a retention expiration date is not transmitted or is outside the Min/Max range.
    - Configuring the inactivity period, if the Autolock feature will be utilized. Cohasset recommends a period of 24 hours or less
  - If **View-level** retention management is applied, setting an appropriate Lock Until date that meets the longest retention period associated with the record objects in the DataLock View. Since a single Lock Until date applies to all record objects in a View, careful planning of the contents for each DataLock View may help prevent excessive retention.
    - Applying any extensions of the Lock Until date to replicated DataLock Views.
    - Managing the original View, which remains available in mutable (changeable) form after the DataLock View is created, to assure any subsequent changes or additions required for regulatory compliance are captured within a new DataLock View.
    - Ensuring regulated record objects are locked, ideally within 24 hours of recording within Cohesity DataPlatform

- Ensuring *DataLock Views* utilized to store regulated record objects reside within a Cohesity Cluster (on premises or in the cloud) to maintain proper retention and deletion controls. These controls do not transfer to other external, non-Cohesity Cluster storage systems.
- Ensuring the record objects required for a legal hold are preserved by extending *Lock Until* dates, as needed. Note: If managing record objects at the View-level, the *Lock Until* date applies to all records in the *DataLock View*. Therefore, this action may result in preserving records that are not required for the Legal Hold.
- Establishing processes to manage retention, legal holds and disposition of replicated locked record objects and *DataLock* Views.
- Configuring the system clock to regularly, e.g., every 5 minutes, synchronize with an external time server, e.g., a network time protocol (NTP) clock.
- Configuring security settings within the DataPlatform environment and establishing processes for ongoing security management.
- Storing record objects requiring event-based retention periods in a separate compliance system, since Cohesity DataPlatform does not currently support event-based retention periods.

2.2 Accurate Recording Process

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

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

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

2.2.2 Compliance Assessment

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

2.2.3 Cohesity DataPlatform Capabilities

Cohesity DataPlatform 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 advanced storage recording technology (such as advanced magnetic storage technology which utilizes multiple inter-component and inter-step, cyclic redundancy checks (CRCs),

as well as write-error detection and correction) are relied upon to ensure that the record objects and Views are written in a high-quality and accurate manner.

- During write activities for each record object, Cohesity DataPlatform utilizes SHA-I and Aldler32 algorithms to calculate a checksum value, which is then stored as system metadata and subsequently used for post-recording verification processes.

Post-Recording Verification

- Integrity of data and system metadata is validated by comparing the checksums via periodic background scans and upon every access.
- If a read error is detected, meaning the integrity check value is invalid, recovery is automatically accomplished by one of the following two methods:
  - Erasure Coding – If erasure coding is configured within a Cluster and an erasure coded segment is determined to be corrupt, the system will automatically regenerate an accurate replica based on the remaining valid segments.
  - Resiliency Factor – Alternatively, if Resiliency Factor is configured within a Cluster, the system will automatically recover the data from a duplicate copy on another storage node.

2.2.4 Additional Considerations

The regulated entity is responsible for configuring Cohesity DataPlatform to utilize either erasure coding or Resiliency Factor to ensure automatic recovery in the event of data corruption.

2.3 Serialize the Original and Duplicate Units of Storage Media

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

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

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

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

2.3.2 Compliance Assessment

It is Cohasset's opinion that the capabilities of Cohesity DataPlatform meet the requirements of the SEC Rule for serializing the original and duplicate copies of the record objects.

2.3.3 Cohesity DataPlatform Capabilities

- The file name and creation (storage) date/time attributes are passed from the source system and stored as part of the record system metadata on Cohesity DataPlatform. Cohesity DataPlatform verifies this data is transmitted and if not, an error message is returned to the user and the record object is not stored. The user must resend the record object, with the required system metadata attributes.
- Cohesity assigns a 64-bit unique identifier to each file and to each View. The system does not allow duplicate identifiers.
- The combination of the unique View and record object (a) name, (b) ID, and (c) creation date/time represent a serialization of the record object in both space and time.

2.3.4 Additional Considerations

There are no additional considerations related to this requirement.

2.4 Capacity to Download Indexes and Records

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

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

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

2.4.2 Compliance Assessment

It is Cohasset's opinion that the capabilities of Cohesity DataPlatform supports the regulated entity in meeting this requirement by providing authorized users direct query access to *DataLock View* and record object system metadata (index attributes), as well as the ability to download record objects and system metadata via NFS, SMB or S3 interfaces. Record objects and system metadata can then be reproduced or transferred by the regulated entity to any compliant media as required.

2.4.3 Cohesity DataPlatform Capabilities

- Cohesity DataPlatform provides search capabilities across *DataLock View* and record object system metadata, e.g. View Name, record object name, and *Lock Until* date.
- Cohesity DataPlatform allows authorized users to access the record objects and system metadata of record objects and *DataLock Views* with NFS, SMB or S3 interfaces.
- Via local capabilities, the record objects and associated system metadata can be searched, viewed, reproduced or transferred to any other compliant storage media; however, the locked record objects stored in the View cannot be modified or deleted.

2.4.4 Additional Considerations

The regulated entity is responsible for (a) authorizing user access, (b) maintaining Cohesity DataPlatform, and (c) assuring that the regulator, self-regulatory organization or designated examining authority receive downloads of the record objects and metadata (index) attributes, in the requested form and medium.

2.5 Duplicate Copy of the Records Stored Separately

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

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

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

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

2.5.2 Compliance Assessment

It is Cohasset's opinion that the capabilities of Cohesity DataPlatform meet the SEC requirement through the use of either 1) erasure coding, whereby record objects are recorded in segments across a minimum of 3 storage nodes, or 2) Resiliency Factor, whereby at least two complete copies of a record object are written to separate nodes. If a record object is determined to be compromised, i.e. lost or damaged, the system will ensure an accurate replica is restored from a duplicate or regenerated from remaining valid erasure coded segments.

2.5.3 Cohesity DataPlatform Capabilities

- Cohesity DataPlatform can be configured to write data to a View using erasure coding. With erasure coding, each replica of the data is recorded in segments onto separate storage nodes within the Cluster, assuring the full regeneration of the record object, should the original become compromised or a storage node is unavailable. The node, disk, offset length, and data value are stored as system metadata for each file stored.
  - A minimum of three storage nodes should be configured to ensure effective use of erasure coding and facilitate the automatic regeneration in the event that a node failure makes the record object inaccessible.
- Alternatively, Cohesity DataPlatform can be configured to write data to a View using Resiliency Factor with a replication factor of two or three. Resiliency Factor ensures a minimum of two full copies of the data exist across different nodes within the same Cluster. In the event a record object is compromised, or a storage node is unavailable, Resiliency Factor automatically recovers a valid copy of the record object from a different node.
- In version 6 of Cohesity DataPlatform, neither erasure coding nor Resiliency Factor is supported across geographically dispersed nodes.
  - Should the regulated entity require geographically dispersed replicas of Views, limited replication capabilities are available as ***a supplement to*** erasure coding or Resiliency Factor. The DataPlatform can be configured to replicate a View to another Cluster, either local or remote, and in the event a record object

in the primary View becomes corrupted, it can manually be restored from the secondary Cluster. However, a regulated entity must be mindful of the following constraints:

File-level DataLock:

- Immutability and retention control codes associated with the source View are carried over to the replicated View, however, there may be delays in propagation based on the configuration established for replication.

View-level DataLock:

- Control codes from a primary *DataLock View* are not carried over to the replicated View, requiring the regulated entity to immediately execute the *DataLock* process on the replicated View and ensure the same *Lock Until* date is applied.
- If a subpoena or legal hold is identified for a View that has been replicated, the *Lock Until* date and *View description* field must be managed on both original and replicated Views.
- Record objects stored in the original and replicated Views are retained for the time-period specified by their respective *Lock Until* dates. Once the *Lock Until* date has expired for the original, both the original and duplicate copy of the View are eligible for deletion. The manual deletion process must be executed on both the original and replicated Views.

2.5.4 Additional Considerations

The regulated entity is responsible for the following:

- Configuring Cohesity DataPlatform to utilize either erasure coding, with a minimum of three storage nodes, or Resiliency Factor.
- Establishing processes to manage retention, legal holds and disposition of replicated *DataLock Views* if geographically dispersed replication is configured on Cohesity DataPlatform as a supplement to erasure coding or Resiliency Factor.

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 Cohesity DataPlatform, utilized with the *DataLock* feature, in comparison to the CFTC requirements.

The individual relevant requirements cited in Section 2, *Assessment of Compliance with SEC Rule 17a-4(f)*, are based on the wording in SEC Rule 17a-4(f) and Cohasset's interpretation of the requirements, given the associated SEC Interpretive Releases. Specifically, the SEC's 2003 Interpretive Release reiterates that the Rule sets forth standards that the electronic storage media must satisfy to be considered an acceptable method of storage under 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 Cohesity DataPlatform capabilities that align with the SEC requirements to the *principles-based* CFTC requirements, it is essential to recognize that the SEC Rule separately describes requirements for index data and audit trail, whereas the CFTC in 17 CFR § 1.31(a) establishes an expanded definition of an electronic regulatory record to include the information as specified in paragraph (i) and (ii) below.

> ***Definitions**. For purposes of this section:*
> *Electronic regulatory records means all regulatory records other than regulatory records exclusively created and maintained by a records entity on paper.*
> *Records entity means any person required by the Act or Commission regulations in this chapter to keep regulatory records.*
> *Regulatory records means all books and records required to be kept by the Act or Commission regulations in this chapter, including any record of any correction or other amendment to such books and records, provided that, with respect to such books and records stored electronically, regulatory records shall also include:*
> *(i) Any data necessary to access, search, or display any such books and records; and*
> *(ii) All data produced and stored electronically describing how and when such books and records were created, formatted, or modified.* [emphasis added]

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

CFTC 1.31(c)-(d) Requirement	Compliance Assessment Relative to CFTC 1.31(c)-(d)	SEC 17a-4(f) Requirements Listed in the Referenced Sections
(c) **Form and manner of retention.** Unless specified elsewhere in the Act or Commission regulations in this chapter, all regulatory records must be created and retained by a records entity in accordance with the following requirements: (1) **Generally.** Each records entity shall retain regulatory records in a form and manner that ensures the *authenticity and reliability* of such regulatory records in accordance with the Act and Commission regulations in this chapter. (2) **Electronic regulatory records.** Each records entity maintaining electronic regulatory records shall establish appropriate systems and controls that ensure the *authenticity and reliability* of electronic regulatory records, including, without limitation: (i) Systems that *maintain* the security, signature, and data as necessary to ensure the *authenticity* of the information contained in electronic regulatory records and to monitor compliance with the Act and Commission regulations in this chapter;	It is Cohasset's opinion that the capabilities described in Sections 2.1 through 2.4 meet CFTC requirements (c)(1) and (c)(2)(i) for record objects. Additionally, for *records stored electronically*, the CFTC has expanded the definition of *regulatory records* in 17 CFR § 1.31(a) to include metadata: *Regulatory records means all books and records required to be kept by the Act or Commission regulations in this chapter, including any record of any correction or other amendment to such books and records, provided that, with respect to such books and records stored electronically, regulatory records shall also include:* *(i) Any data necessary to access, search, or display any such books and records; and* *(ii) All data produced and stored electronically describing how and when such books and records were created, formatted, or modified.* [emphasis added] It is Cohasset's opinion that the record object system metadata, e.g., unique identifier, creation date and time, and other immutable metadata (index attributes) are retained as an integral part of the record object; and, therefore are subject to the same retention protections as the associated record object. To satisfy this requirement for other essential data related to how and when the record objects were created, formatted, or modified, the regulated entity must retain this data in a compliant manner.	Section 2.1 *Non-Rewriteable, Non-Erasable Record Format* *Preserve the records exclusively in a non-rewriteable, non-erasable format.* [SEC 17a-4(f)(2)(ii)(A)] Section 2.2 *Accurate Recording Process* *Verify automatically the quality and accuracy of the storage media recording process.* [SEC 17a-4(f)(2)(ii)(B)] Section 2.3 Serialize the Original and Duplicate Units of Storage Media *Serialize the original and, if applicable, duplicate units of storage media, and time-date for the required period of retention the information placed on such electronic storage media.* [SEC 17a-4(f)(2)(ii)(C)] *Section 2.4 Capacity to Download Indexes and Records* *Have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable under this paragraph (f) as required by the Commission or the self-regulatory organizations of which the member, broker, or dealer is a member.* [SEC 17a-4(f)(2)(ii)(D)]
(ii) Systems that ensure the records entity is able to produce electronic regulatory records[5] in accordance with this section, and *ensure the availability of such regulatory records in the event of an emergency or other disruption* of the records entity's electronic record retention systems; and	It is Cohasset's opinion that the capabilities described in Section 2.5 meet this requirement for the record object content and associated system metadata, e.g., unique identifier and creation date and time. 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 2.5 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)]
(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

[5] 17 CFR § 1.31(a) includes indices (*Any data necessary to access, search, or display any such books and records*) in the definition of regulatory records.

CFTC 1.31(c)-(d) Requirement	Compliance Assessment Relative to CFTC 1.31(c)-(d)	SEC 17a-4(f) Requirements Listed in the Referenced Sections
(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 Cohesity DataPlatform 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 Cohesity DataPlatform to retrieve and download the record objects and the system metadata retained by Cohesity DataPlatform. 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. When additional data related to how and when the record objects were created, formatted, or modified is requested, 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 Cohesity DataPlatform version 6, utilized with the *DataLock* feature, in comparison to the five requirements related to recording, storage and retention of record objects and associated metadata, set forth in SEC Rule 17a-4(f) and its associated Interpretive Releases. Cohasset also correlated the principles-based requirements in CFTC Rule 1.31(c)-(d) to the assessed capabilities of Cohesity DataPlatform.

Cohasset determined that Cohesity DataPlatform, utilized with the *DataLock* feature, 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 retention periods.
- Prohibits deletion of a record object and its system metadata until the associated retention period has expired.
- Allows the retention period to be extended to address special circumstances, such as litigation or subpoena.
- Verifies the accuracy and quality of the recording process automatically, utilizing (a) advanced storage recording technology, and (b) a checksum that is calculated during the recording process and is stored as a system metadata attribute and utilized for post-recording verification.
- Uniquely identifies and chronologically serializes each stored record object.
- Provides search capabilities across View and record object system metadata, e.g. View Name, record object name, and *Lock Until* date.
- Allows authorized users to access the record objects and system metadata with NFS, SMB or S3 interfaces for local reproduction or transfer to a format and medium acceptable under the Rule.
- Recovers an accurate copy of a record object and metadata (including index attributes) from a duplicate, should it become lost or damaged, or regenerates an accurate replica from valid erasure coded segments.

Accordingly, it is Cohasset's opinion that Cohesity DataPlatform version 6.0, when properly configured and utilized with the *DataLock* feature to store and retain time-based records, meets the requirements that relate directly to the recording, storage and retention of record objects and system metadata.

5 | Overview of Relevant Regulatory Requirements

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

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

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

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

- The Rule itself, as modified over time by the SEC. These modifications to the original Rule have not affected the requirements for electronic storage media, which are the basis of this assessment. However, certain Interpretive Releases have clarified the context and meaning of certain requirements and conditions of the Rule.
- SEC Interpretive Release No. 34-44238, *Commission Guidance to Broker-Dealers on the Use of Electronic Storage Media under the Electronic Signatures in Global and National Commerce Act of 2000 with Respect to Rule 17a-4(f)*, dated May 1, 2001 (the "2001 Interpretive Release").
- SEC Interpretive Release No. 34-47806, *Electronic Storage of Broker-Dealer Records*, dated May 7, 2003 (the "2003 Interpretive Release").

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

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

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

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

> *to be retained. The amendments reflect a recognition of technological developments that will provide economic as well as time-saving advantages for broker-dealers by expanding the scope of recordkeeping options while at the same time continuing to require broker-dealers to maintain records in a manner that preserves their integrity. The Commission is also issuing an interpretation of its record preservation rule relating to the treatment of electronically generated communications.*
> ***
> ***II. Description of Rule Amendments***
> ***A. Scope of Permissible Electronic***
> ***Storage Media***
> ****The Commission is adopting a rule today which, instead of specifying the type of storage technology that may be used, sets forth standards that the electronic storage media must satisfy to be considered an acceptable method of storage under Rule 17a–4. Specifically, because optical tape, CD–ROM, and certain other methods of electronic storage are available in WORM and can provide the same safeguards against data manipulation and erasure that optical disk provides, the final rule clarifies that broker-dealers may employ any electronic storage media that meets the conditions set forth in the final rule.*[6] [emphasis added]

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

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

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

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

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

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

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

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

> *Moreover, there may be circumstances (such as receipt of a subpoena) where a broker-dealer is required to maintain records beyond the retention periods specified in Rule 17a-4 or other applicable Commission rules. Accordingly, a broker-dealer must take appropriate steps to ensure that records are not deleted during periods when the regulatory retention period has lapsed but other legal requirements mandate that the records continue to be maintained, and the broker-dealer's storage system must allow records to be retained beyond the retentions periods specified in Commission rules. [emphasis added]*

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

See Section 2, Assessment of Compliance with SEC Rule 17a-4(f), for a list of the *five* SEC requirements relevant to the recording, storage and retention of electronic records and a description of the capabilities of Cohesity DataPlatform 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[7] and event-time-based[8] 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 Cohesity DataPlatform related to each requirement, see Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*.

[7] 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.

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

About Cohasset Associates, Inc.

Cohasset Associates, Inc. (www.cohasset.com) is recognized as a leading professional consulting firm, specializing in records management and information governance. Drawing on more than forty years of experience, Cohasset provides its clients with innovative advice on managing their electronic information as the digital age creates operational paradigms, complex technical challenges and unprecedented legal issues.

Cohasset provides award-winning professional services in four areas: management consulting, education, thought-leadership and legal research.

Management Consulting: Cohasset strategizes with its multi-national and domestic clients, engaging in implementation activities to promote interdisciplinary information governance, achieve business objectives, optimize information value, improve compliance, and mitigate information-related risk.

Cohasset has been described as *the only management consulting firm in its field with its feet in the trenches and its eye on the horizon*. This fusion of practical experience and vision, combined with a commitment to excellence, results in Cohasset's extraordinary record of accomplishments.

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

For domestic and international clients, Cohasset:

- *Formulates information governance implementation strategies*
- *Develops policies and standards for records management and information governance*
- *Creates clear and streamlined retention schedules*
- *Prepares training and communications for executives, the RIM network and all employees*
- *Leverages content analytics to improve lifecycle controls for large volumes of eligible information, enabling clients to classify information, separate high-value information and delete what has expired*
- *Designs and assists with the implementation of information lifecycle practices that avoid the cost and risk associated with over-retention*
- *Defines technical and functional requirements and assists with the deployment of enterprise content management and collaboration tools*

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

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