Cohasset Associates

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

# MinIO Object Storage

## Abstract


MinIO Object Storage is an open-source, software-defined, high performance object storage system that is designed for private cloud environments. It runs on industry standard hardware. The Object Lock features are designed to meet securities industry requirements for preserving records in a non-rewriteable, non-erasable format, for objects stored with the *Object Lock* mode set *Compliance*.

In this Report, Cohasset Associates, Inc. (Cohasset) assesses the capabilities of MinIO Object Storage (see Section 1.3, *MinIO Object Storage Overview and Assessment Scope*) relative to:

- The recording and non-rewriteable, non-erasable storage requirements for electronic records, as specified by:
  - 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).
- The principles-based electronic records requirements of the Commodity Futures Trading Commission (CFTC) in 17 CFR § 1.31(c)-(d), which regulates commodity futures trading.

It is Cohasset's opinion that MinIO Object Storage, Release 172, when properly configured and when *Object Lock* mode is set to *Compliance*, retains records requiring time-based retention, in compliance with the recording and non-rewriteable, non-erasable storage of electronic records of SEC Rule 17a-4(f) and FINRA Rule 4511(c). Additionally, the assessed capabilities of MinIO Object Storage meet the principles-based requirements of CFTC Rule 1.31(c)-(d).


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 Rule 17a-4(f), as defined by 1) the No Action Letter in 1993 (allowing broker dealers to use non-rewriteable, non-erasable digital storage media); 2) the issuance of the Rule in 1997; and 3) the Interpretive Release in 2003, which authorizes the use of erasable storage, conditioned on integrated control codes, to prevent premature deletion of records.

# Table of Contents

# 1 | Introduction

*Regulators, world-wide, establish explicit requirements for regulated entities that elect to retain books and records[1] on electronic storage media. Given the prevalence of electronic books and records, these requirements apply to most broker-dealer and commodity futures trading firms and other organizations with similarly regulated operations.*

*This* Introduction *briefly summarizes the regulatory environment pertaining to this assessment, explains the purpose and approach for Cohasset's assessment, and provides an overview of MinIO Object Storage and the scope of this assessment.*

## 1.1 Overview of the Regulatory Requirements

### *1.1.1 SEC Rule 17a-4(f) Requirements*

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

> *The Commission is adopting a rule today which, instead of specifying the type of storage technology that may be used, sets forth standards that the electronic storage media must satisfy to be considered an acceptable method of storage under Rule 17a–4.*[2] [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).

For additional information, refer to Section 5.1, *Overview of SEC Rule 17a-4(f) Electronic Records Storage Requirements*.

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

[2] Exchange Act Release No. 38245 (Feb. 5, 1997), 62 FR 6470 (Feb. 12, 1997) ("Adopting Release").

### *1.1.3 CFTC Rule 1.31(c)-(d) Requirements*

Effective August 28, 2017, 17 CFR § 1.31 (the CFTC Rule), the Commodity Futures Trading Commission (CFTC) promulgated principles-based requirements for organizations electing to retain electronic regulatory records. These amendments modernize and establish technology-neutral requirements for the *form and manner of retention* and the *inspection and production* of regulatory records.

Refer to Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*, which correlates the CFTC principles-based requirements to the capabilities of MinIO Object Storage with *Object Lock*. Additionally, refer to Section 5.3, *Overview of CFTC Rule 1.31(c)-(d) Electronic Regulatory Records Requirements*.

## 1.2 Purpose and Approach

To obtain an independent and objective assessment of the compliance capabilities of MinIO Object Storage, MinIO 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.

MinIO engaged Cohasset to:

- Assess the capabilities of MinIO Object Storage in comparison to the five requirements of SEC Rule 17a-4(f) for the recording and non-rewriteable, non-erasable storage of electronic records; see Section 2, *Assessment of Compliance with SEC Rule 17a-4(f);* and
- Associate the principles-based requirements of CFTC Rule 1.31(c)-(d) to the assessed capabilities of MinIO Object Storage; 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.*

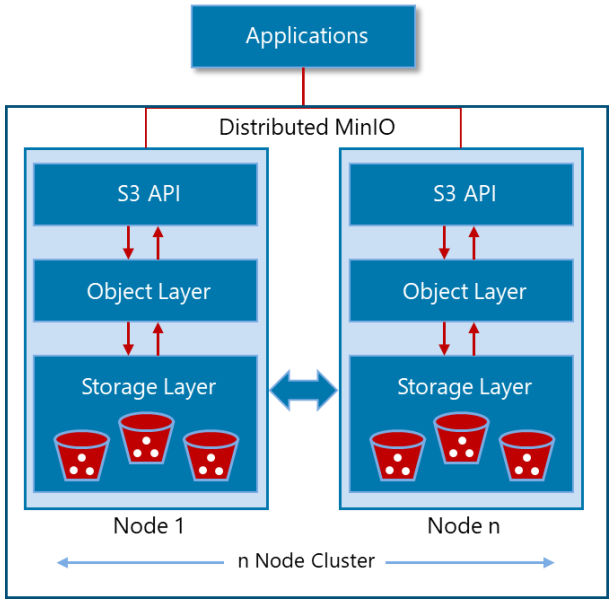
This assessment represents the professional opinion of Cohasset and should not be construed as either an endorsement or a rejection, by Cohasset, of MinIO Object Storage and its capabilities or other MinIO products or services. The information utilized by Cohasset to conduct this assessment consisted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

MinIO Object Storage is a high performance, distributed, private cloud object storage system that is designed for compatibility with the Amazon Simple Storage Service (S3) protocol. The MinIO Object Storage environment runs on industry standard hardware and is fully open source. MinIO supports traditional object storage, such as secondary storage, disaster recovery and archiving as well as modern use cases, such as advanced analytics, AI (artificial intelligence)/ML (machine learning) and high-performance primary storage for Kubernetes environments.

The MinIO Object Storage architecture (illustrated in the diagram) consists of the following components:




- The **S3 APIs** (application programming interface) natively support Amazon S3 APIs, which can be used for data management, collaboration and archiving.
- ***Object Layer*** performs erasure code, bitrot check, and encryption functions.
- ***Storage Layer*** is responsible for storing and retrieving objects, stored in Buckets, from physical media.
- ***Node*** is an instance of a MinIO Server.
- **Node Cluster** is an unlimited collection of distributed Nodes.
- ***Buckets*** are cluster spanning logical containers that store record objects, including individual versions of a given record object. Each object consists of the content and its descriptive metadata.

Cohasset assessed the capabilities of MinIO Object Storage, Release 172, configured with *Object Lock* enabled and *Object Lock mode* set to *Compliance,* when on-premises, running on MinIO qualified hardware.

Note: Deploying MinIO in Gateway mode or on public cloud storage are outside of the scope of this Assessment Report.

The following section documents Cohasset's assessment of MinIO, relative to the pertinent requirements in SEC Rule 17a-4(f). Throughout this report, the above described operating environment of MinIO will be assessed.

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

*This section presents Cohasset's assessment of the capabilities of MinIO Object Storage for compliance with the five requirements related to the recording and non-rewriteable, non-erasable storage 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 MinIO Object Storage
- ***MinIO Object Storage Capabilities*** – Description of relevant capabilities
- ***Additional Considerations*** – Additional considerations related to meeting the specific requirement

The following subsections document Cohasset's assessment of the capabilities of MinIO Object Storage, as described in Section 1.3, *MinIO Object Storage Overview and Assessment Scope*, relative to each pertinent requirement of SEC Rule 17a-4(f).

## 2.1 Non-Rewriteable, Non-Erasable Record Format

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

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

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

The following statement in the 2003 Interpretive Release further clarifies that certain implementations of rewriteable and erasable media, such as magnetic disk or magnetic tape, meet the requirements of a non-rewriteable and non-erasable 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 features of MinIO Object Storage, with *Object Lock* enabled on the bucket and record objects stored in *Compliance Mode*, meet this SEC requirement to retain records in non-rewriteable, non-erasable format for time-based[3] retention periods and any applied legal holds, when (a) properly configured, as described in Section 2.1.3, and (b) the considerations described in Section 2.1.4 are satisfied.

### *2.1.3 MinIO Object Storage Capabilities*

This subsection describes the capabilities of MinIO Object Storage that pertain to this SEC requirement for preserving electronic records (record objects) in a format that is non-rewritable and non-erasable, for the required retention period and any associated legal holds.

*Overview*

- To meet the non-rewriteable, non-erasable requirements of SEC Rule 17a-4(f), a record requiring time-based retention, must (a) be stored in a Bucket with the *Object Lock* feature *enabled*, (b) have the *Object Lock mode* set to *Compliance (*hereinafter *Compliance Mode)*, and (c) have a *Retain Until Date* applied to each record object (version). With this configuration, MinIO disables all application programming interfaces (APIs) that could potentially alter or prematurely delete the record object and immutable metadata.
- Object Lock mode may be set, either (a) explicitly by the user/API, or (b) implicitly by inheriting the default values configured for the bucket.
- In addition to *Compliance Mode*, MinIO *Object Lock* offers *Governance Mode*, which allows authorized users to remove *Object Lock* from an object. Therefore, only *Compliance Mode* meets the requirements of the Rule.
- When litigation or a subpoena requires record objects to be placed on hold, which could entail retention beyond the assigned retention period, a *Legal Hold* status may be applied to the record objects. This prohibits deletion of the record objects until the *Legal Hold* status is removed.

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

The fundamental features of MinIO Object Storage prevent changes or modifications to record objects and associated immutable metadata, once stored. Further, when the above configurations and settings are applied:

- The *Object Lock* feature cannot be removed from a Bucket that contains record objects.
- When *Compliance Mode* is set, on the record object, it cannot be removed, and prevents the specified *Retain Until Date* from being shortened or removed. It can only be extended, if necessary.
- The record object and its immutable metadata cannot be modified, overwritten or deleted until both (a) the *Retain Until Date* has expired and (b) the *Legal Hold* status is removed.

### *MinIO Bucket and User Policy Configurations*

- For each Bucket retaining record objects requiring compliance with SEC Rule 17a-4(f), the *Object Lock* feature must be *enabled* when the bucket is created. Enabling *Object Lock* automatically enables the *Versioning* feature. Once the *Object Lock* feature is enabled, it cannot be suspended or disabled.
- Optionally, Bucket default values may be set for (a) *Object Lock* mode, (b) *Default retention duration* (e.g., 6 Years), and (c) *Minimum and Maximum* retention durations. Once configured, these defaults automatically apply to each stored record object and metadata, unless retention controls are explicitly transmitted with the record object.
  - *Object Lock mode* and the *Default retention period* must be configured together or neither default can be configured.
    - The default *Object Lock mode* may be set to must be set to *Compliance*, for record objects requiring compliance with SEC Rule 17a-4(f)
    - The *Default retention duration* is added to the storage date to calculate the record object's *Retain Until Date*. (See section *Record Object Definition and Retention Controls*, for more information).
  - The Bucket *Minimum and Maximum retention durations* only apply to anonymous users. Known users are governed by the *User Policy Minimum and Maximum* retention durations, described in the following paragraph.
- *User Policies*, configured via the S3 API, define a set of permissions that grant access to actions and resources in MinIO Object Storage. Optionally, a *User Policy* may constrain the user (e.g., source application) to an *explicit* minimum and maximum range for the applied *Retain Until Dates*.
  - Since the *Minimum and Maximum retention range* is set through the *User Policy*, each permissioned user of a Bucket may be bound by a different *Minimum and Maximum* range. If a user attempts to set retention outside of this range, the request is denied.
    - Authorized users may change the *Minimum and Maximum* range at any time. The updated *Minimum and Maximum* applies to new record objects and does not apply to previously stored record objects.
  - IMPORTANT NOTE: When a record object is not transmitted with an explicit *Retain Until Date,* either (a) the object is stored without any retention controls (if no Bucket defaults were configured) or (b) the

Bucket *Default retention period* is applied to the record object even if the default is outside the *Minimum and Maximum* range for the user, thus overriding the policy. Therefore, setting the *Default retention period* requires careful planning to assure an appropriate *Retain Until Date* is set, when an explicit *Retain Until Date* is not transmitted with the record object.

### *Record Object Definition and Retention Controls*

- Each record object is comprised of:
  - Complete content of the record object,
  - Immutable Metadata, which includes, but is not limited to, unique object *Key* name, version identifier (*VersionID*), creation/storage (last modified) date and time, object size, and user-defined custom metadata (key-value pairs), and
  - Mutable Metadata, which includes Retain Until Date, Object Lock mode and Legal Hold status
- Each record object has a separate *Retain Until Date* and *Object Lock* mode either transmitted with it or inherited from Bucket default values. (REMINDER: The term record object is defined as a version of a record object.)
- The *Object Lock* mode can be set to one of three options (*null*, *Governance* or *Compliance*) for a given record object and its metadata; **only** *Compliance Mode* meets the requirements of SEC Rule 17a-4(f).
  1. *Object Lock mode* set to *Compliance,* assures the following retention controls:
     - The *Retain Until Date* may be extended to a future date but cannot be shortened or cleared by any user, including the account root user.
     - The *Object Lock mode* cannot be changed to *Governance* or cleared (*null*) by any user, including the account root user.
  2. *Object Lock mode* set to *Governance,* permits clearing the *Object Lock* mode and the *Retain Until Date*. As a result, *Governance* is disallowed for record objects required to comply with the Rule.
  3. *Object Lock mode* may be *null (blank),* which does not apply any retention controls and, therefore, is disallowed for records required to comply with the Rule.
- The following MinIO Object Store features prevent modification, overwrite and deletion, until eligible:
  - The fundamental capabilities of *Compliance Mode*, when enabled, immutably stores record objects and immutable metadata.
  - The *Versioning* feature ensures record objects are not overwritten; instead, a new version is created.
  - Each record object is protected from deletion when either:
    - The *Retain Until Date* of the record object has a future date, or
    - The *Legal Hold* status of the record object is enabled (On).
  - For record objects stored in *Compliance Mode,* the *Retain Until Date* may be extended to a future date but cannot be shortened or cleared, by any user, including the account root user.

- To apply *Compliance Mode* and a *Retain Until Date* to the record object, as required to comply with the Rule, either: (a) the source application transmits *Compliance Mode* and an explicit *Retain Until Date* with a record object, or (b) Bucket defaults apply *Compliance Mode* and a D*efault retention duration* for record objects that are transmitted without retention values,.
- A record object may be copied between Buckets, resulting in the creation of a new copy with its own unique metadata. The copy does not retain the original record object's *Retain Until Date*, *Object Lock mode* and *Legal Hold* status; therefore, the attributes need to be set via Bucket defaults or explicitly. The original record object and metadata will remain, unaltered, in the original Bucket.
- The following user actions are rejected, when *Object Lock mode* is set to *Compliance*:
  - Shorten or remove a record object's *Retain Until Date* in *Compliance Mode*.
  - Change the *Object Lock mode* from *Compliance* to *Governance* or from *Compliance* to *null* (blank).
  - Delete a record object, by *VersionID*, before the *Retain Until Date* has passed (expired).

### *Legal Hold*

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

- The *Legal Hold* status (On/Off) may be applied to any record object stored in a Bucket with the *Object Lock* feature *enabled*.
  - Each record object version includes a separate *Legal Hold* status attribute.
  - The *Legal Hold* status is independent of the record object's *Retain Until Date* and *Object Lock* mode; therefore, a *Legal Hold* status may be applied to any record object in a Bucket with the *Object Lock* feature *enabled*, including record objects without a *Retain Until Date* and *Object Lock* mode.
  - When the *Legal Hold* status is set (On), it prohibits deleting the record object until the *Legal Hold* status is removed (Off).
  - When the *Legal Hold* status is cleared (Off), this attribute no longer mandates preservation of the record object; however, the retention controls continue to apply to the record object.
- The *Legal Hold* status for a record object can be verified by either: (a) using *Stat* command to view the metadata for the object or (b) issuing 'get-object-legal hold' through the S3 API.

### *Managing Versions*

- Enabling the *Object Lock* feature for a Bucket automatically enables the *Versioning* feature.
- When the versioning feature is enabled, each version of the record object is separately managed, in accordance with the following controls:
  1. A new version is created when the file contents or metadata are changed or when a new file (with the same *Key* name) is uploaded.

2. A new version is not created when retention controls (*Object Lock mode* and *Retain Until date*) are applied or when the *Legal Hold* status is applied or removed for a stored version of the record object.
3. The retention controls use the version creation/storage date and time:
   - When the Bucket *Default retention duration* is applied to the version, it is added to the creation/storage date and time to calculate the *Retain Until date* for the version.
   - When a *Minimum and Maximum* range applies, the version creation/storage date and time is used for the validation.
4. Deleting a record object version by *Key* name without specifying a *VersionID* creates a 'delete marker', which is then considered the most recent version. The 'delete marker' does not affect the stored versions of the record. The 'delete marker' may be deleted in the future.
5. When attempting to delete a record object by *VersionID*, Compliance Lock protections apply, and only eligible versions are deleted. An error message is communicated, and the deletion operation fails, if the version is ineligible for deletion.

### *Deletion Controls*

- The *Retain Until Date* and *Legal Hold* status determine if the record object is eligible for deletion (eligibility for deletion does not cause automatic deletion). The following criteria must be met for a record object to be eligible for deletion:
  - The *Retain Until Date* must have expired (date prior to current date).
  - The *Legal Hold* status must be clear (Off).
- The Bucket cannot be deleted, until it is empty.

### *Clock Management*

- To meet the requirements of the Rule, Cohasset asserts that every system clock must synchronize to an external time server, e.g., a network time protocol (NTP) clock. The MinIO Object Storage system must be configured to enable NTP and regularly check the time of the external source (NTP) and resynchronize time.
  - When *Object Lock* is *enabled*, MinIO Object Storage prohibits updating the system clock locally. These controls prevent or correct any inadvertent or intentional administrative modifications of the time clock, which could allow for premature deletion of record objects.

### *Security*

- MinIO Object Storage is designed to meet Enterprise security and compliance requirements. MinIO Object Storage supports the following server-side encryption schemes to protect data at rest and in motion:
  - Encryption is supported using AES-256-GCM and ChaCha20-Poly1305.
  - Encrypted objects are tamper-proofed with AEAD server-side encryption.
  - MinIO Object Storage is compatible with commonly used Key Management solutions (e.g., HashiCorp Vault).

- MinIO Object Storage uses a key management-system (KMS) to support SSE-S3. If a client requests SSE-S3, or auto-encryption is enabled, the MinIO Object Storage server encrypts each object with a unique object key which is protected by a master key managed by the KMS.
- MinIO Object Storage may be configured to protect data in-transit (data traveling to and from MinIO Object Storage) may be protected using Secure Sockets Layer (SSL).
- Roles-based Security (RBAC) is employed by MinIO Object Storage. The user is identified by access key and policy to allow S3 API (Application Programming Interface) calls. The permissions for each user are controlled through User Policies.

### *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:

- Assigning permissions required to manage the retention controls and properly configuring the User Policies and MinIO Object Store Buckets that will retain regulated records. NOTE: Cohasset recommends setting Bucket defaults: (a) Object Lock in *Compliance Mode* and (b) an appropriate retention period that complies with the regulatory retention requirements.
- Optionally, setting *Minimum and Maximum retention durations* for the Bucket (which apply to anonymous users) or for *User Policies,* to validate the *Retain Until Date* applied to each record object.
- Applying the retention controls to each record object that is required for regulatory compliance.
  - Setting the *Object Lock mode* to *Compliance*
  - Applying a *Retain Until Date* that meets regulatory retention requirements

  Cohasset recommends that retention controls be applied within 24 hours of storing a record object required for compliance with the Rule:
- Setting a Legal Hold status to On, when required, to preserve record objects for legal matters, government investigations, external audits and other similar circumstances. NOTE: The Legal Hold status should be set to Off, when preservation is no longer required.
- Limiting the creation and management of 'delete markers.' NOTE: Cohasset recommends always specifying the *VersionID* in delete requests.
- Storing record objects requiring event-based[4] retention periods in a separate compliance system, since MinIO Object Storage does not currently support event-based retention periods.
- Setting appropriate security controls to (1) restrict network ports and protocol access, (2) establish roles-based access, and (3) encrypt data in transit and while at rest.

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

## 2.2 Accurate Recording Process

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

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

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

### 2.2.2 Compliance Assessment

Cohasset affirms that the capabilities of MinIO Object Storage, in conjunction with the inherent capabilities of advanced magnetic storage technology, meet this SEC requirement for accurate recording and post-recording verification.

### 2.2.3 MinIO Object Storage Capabilities

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

*Recording Process:*

- An MD5 checksum must be transmitted with the record object. The record object will be stored only if the MD5 checksum value calculated by MinIO Object Storage matches the uploaded checksum. If it does not match, an error is reported, and the record object must be re-uploaded.
- MinIO Object Storage utilizes advanced electronic recording technology which applies a combination of checks and balances to assure that record objects are written in a high quality and accurate manner.
- Each record object and associated metadata is protected with erasure code and a bit rot hash.

*Post-Recording Verification Process:*

- MinIO Object Storage uses erasure coding to split the record object into data segments (chunks) and assigns a checksum to each segment. Integrity of the record object is validated by comparing the checksum of each segment during read, to ensure that an accurate record object is delivered.
- MinIO Object Storage employs a background healing process that scans the data segments, checking and correcting errors. If a segment is corrupt, meaning the checksum value is invalid, an automatic recovery process is initiated to rebuild the segment from the other valid segments.
  - MinIO Object Storage allows the administrator to manually heal (correct) errors, although auto-healing is utilized when possible.

### 2.2.4 Additional Considerations

There are no additional considerations related to this requirement.

## 2.3 Serialize the Original and Duplicate Units of Storage Media

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

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

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

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

### 2.3.2 Compliance Assessment

It is Cohasset's opinion that the capabilities of MinIO Object Storage meet this SEC requirement to serialize the original and duplicate records.

### 2.3.3 MinIO Object Storage Capabilities

- Each record object is serialized in MinIO Object Storage Buckets using a combination of: (a) unique object *Key* name, (b) *VersionID,* and (c) creation/storage date and time stamp. These attributes are immutable.
  - The object name must be unique within the Bucket.
  - The *VersionID* is automatically assigned.
  - The creation/storage date (last modified) date and time is system-defined, immutable, and stored with each record object.
- This combination of unique object *Key* name, *VersionID,* and creation/storage date and time serializes each record object in both space and time.

### 2.3.4 Additional Considerations

There are no additional considerations related to this requirement.

## 2.4 Capacity to Download Indexes and Records

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

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

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

### 2.4.2 Compliance Assessment

It is Cohasset's opinion that the capabilities of MinIO Object Storage meet this SEC requirement to readily download records and indexes (metadata attributes), when the considerations described in Section 2.4.4 are addressed.

### 2.4.3 MinIO Object Storage Capabilities

- MinIO Object Storage users with administrative permissions can find objects and associated metadata using Linux commands which have been expanded to cover governance features.
  - Search functionality is limited to the name of the record object, *VersionID* or list all objects.
  - Metadata is not searchable; however, the *stat* command can be utilized to list metadata.
  - For advanced search capabilities, metadata can be inserted into a custom database and then used to filter basic metadata and head attributes
- Record objects and indexes (metadata attributes) may be downloaded using the S3 API. The following capabilities support the capacity to download record objects and index data (metadata attributes) using the S3 API:
  - List record objects including all versions, including delete markers, in a Bucket (selection criteria based on name may be refined to find and return a subset of the objects in a Bucket).
  - Download selected record objects and the associated indexes (metadata attributes) to a designated storage location.

### 2.4.4 Additional Considerations

The regulated entity is responsible for (a) ensuring record objects with delete markers are included in the search results, (b) authorizing user permissions, (c) maintaining hardware and software to access MinIO Object Storage, (d) assuring that the regulator, self-regulatory organization or designated examining authority receive downloads of the requested record objects and associated indexes (metadata attributes), in the requested format and medium.

## 2.5 Duplicate Copy of the Records Stored Separately

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

**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

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

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

### 2.5.2 Compliance Assessment

Cohasset asserts that MinIO Object Storage meets this SEC requirement for a persistent duplicate copy of the record objects, when (a) properly configured, as described in Section 2.5.3, and (b) the considerations described in Section 2.5.4 are satisfied.

### 2.5.3 MinIO Object Storage Capabilities

There are two options for meeting the conditions of this requirement to separately store a duplicate copy.

*Duplicate Using Erasure Coding*

- MinIO Object Storage uses erasure coding (EC) to store data segments (chunks) of record objects redundantly across multiple nodes. In the event of a disk or node failure, the original record object can be regenerated from redundant data segments.
  - MinIO creates erasure-coding sets of 4 to 16 drives per set.
  - Each object is written to a single erasure coding set, and therefore, is spread over no more than 16 drives.
  - A record object is regenerated from the erasure encoded data.
  - The erasure coded data segments are retained for the full retention period and any applied Legal Holds.

*Duplicate Using Mirror*

- Duplicate copies may be stored using the *Mirror* functionality, which provides continuous synchronization at the Bucket level.
  - When mirroring is configured it copies the default lock configuration from the source bucket.
  - Watch flag identifies changes in the source bucket and copies the changes to the destination bucket. If the destination bucket is unavailable, it will continue to retry until the copy is completed.
  - Scheduled jobs collect source bucket changes not processed and copies the changes to the destination bucket to ensure synchronization.
  - When Object Lock or Legal Hold is added to record objects in the source bucket, an event is triggered to apply these controls to the object on the destination server.

### 2.5.4 Additional Considerations

The regulated entity is responsible for the following.

- When using Mirror functionality, ensure that a scheduled job is configured to run, at a minimum daily, to collect any non-replicated changes on the source bucket and copy the changes to the destination bucket.
- When relying exclusively on erasure coding for the duplicate copy, Cohasset *recommends* the regulated entity configure the system such that the storage pools are equally distributed across three or more geographically dispersed data centers.

# 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 MinIO Object Storage, as described in Section 1.3, *MinIO Object Storage Overview and Assessment Scope*, in comparison to the CFTC requirements.

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

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

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

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

When comparing the capabilities of MinIO Object Storage 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 focus of Cohasset's assessment, presented in Section 2, pertains to MinIO Object Storage, when *Object Lock mode* is set to *Compliance,* which is highly restricted and assures that the storage solution applies controls to (a) protect immutability of the record content and certain system metadata and (b) prevent deletion over the applied retention period.

In the following table, Cohasset correlates the capabilities of MinIO Object Storage, when *Object Lock mode* is set to *Compliance,* to the *principles-based* CFTC requirements related to the *form and manner of retention* and the *inspection and production of regulatory records*. In addition, Cohasset contends that MinIO Object Storage, with record objects stored in *Governance Mode* (which is less restrictive), meets these *principles-based* CFTC requirements, when the regulated entity applies appropriate procedural controls to oversee operations that may allow content to be modified or deleted prior to expiration of the retention period. This less restrictive *Governance Mode* option provides flexibility to remove retention controls, which may be beneficial for compliance with privacy and data protection requirements.

The left-hand column lists the *principles-based* CFTC requirements. The middle column provides Cohasset's analysis and opinion regarding the ability of MinIO Object Storage, with Object Lock to meet the requirements for electronic regulatory records in CFTC Rule 1.31(c)-(d). In addition, for ease of reference, the right-hand column lists the correlated SEC requirements.

| 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:<br>(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.<br>(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:<br>(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 MinIO Object Storage capabilities, when *Object Lock mode* is set to *Compliance*, as described in Sections 2.1 through 2.4 meet CFTC requirements (c)(1) and (c)(2)(i) for record objects.<br>Additionally, for *records stored electronically*, the CFTC has expanded the definition of *regulatory records* in 17 CFR § 1.31(a) to include metadata:<br>*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:*<br>*(i) Any data necessary to access, search, or display any such books and records; and*<br>*(ii) All data produced and stored electronically describing how and when such books and records were created, formatted, or modified.* [emphasis added]<br>● It is Cohasset's opinion that MinIO Object Storage, when *Object Lock mode* is set, retains certain immutable metadata (index attributes) as an integral part of the record object; and, therefore are subject to the same retention controls as the associated record object. Immutable record object metadata includes object Key name, VersionID, creation/storage (last modified) date and time, and user-defined custom metadata (key-value pairs).<br>● Additionally, mutable (changeable) metadata attributes stored for a record object include retention controls and Legal Hold status. The most recent values of mutable metadata are retained for the same time period as the associated record object.<br>● 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***<br>*Preserve the records exclusively in a non-rewriteable, non-erasable format.* [SEC 17a-4(f)(2)(ii)(A)]<br>**Section 2.2 *Accurate Recording Process***<br>*Verify automatically the quality and accuracy of the storage media recording process.* [SEC 17a-4(f)(2)(ii)(B)]<br>**Section 2.3 Serialize the Original and Duplicate Units of Storage Media**<br>*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)]<br>***Section 2.4 Capacity to Download Indexes and Records***<br>*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)] |

| 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 |
|---|---|---|
| (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 MinIO Object Storage capabilities described in Section 2.5, including four options for duplicating the record objects, meet the CFTC requirements (c)(2)(ii) to *ensure the availability of such regulatory records in the event of an emergency or other disruption of the records entity's electronic record retention systems*.<br>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***<br>*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:<br>(1) *Inspection*. All regulatory records shall be open to inspection by any representative of the Commission or the United States Department of Justice.<br>(2) *Production of **paper** regulatory records*. ***<br>(3) *Production of **electronic** regulatory records*.<br>(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.<br>(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.<br>*(4) Production of **original** regulatory records.* *** | It is Cohasset's opinion that MinIO Object Storage 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).<br>Specifically, it is Cohasset's opinion that Section 2.4, *Capacity to Download Indexes and Records*, describes use of MinIO Object Storage to retrieve and download the record objects and the system metadata retained by MinIO Object Storage. 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.<br>If the regulator requests additional data related to how and when the record objects were created, formatted, or modified, the regulated entity will need to provide this information from appropriate source systems | ***Section 2.4 Capacity to Download Indexes and Records***<br>*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 MinIO Object Storage, Release 172, when *Object Lock* mode is set to *Compliance*, in comparison to the five requirements related to the recording and non-rewriteable, non-erasable storage of electronic records, as set forth in SEC Rule 17a-4(f) and its associated Interpretive Releases. (See Section 1.3, *MinIO Object Storage Overview and Assessment Scope*.)

Cohasset determined that MinIO Object Storage, when properly configured, has the following capabilities, which meet the regulatory requirements:

- Maintains record objects and certain record object metadata in a non-erasable and non-rewriteable format for time-based retention periods, when a *Retain Until Date* is applied and the *Object Lock* mode is set to *Compliance*.
- Prohibits deletion of a record object and its immutable metadata until the applied *Retain Until Date* has expired.
- Allows a *Legal Hold* status to be applied to record objects subject to preservation requirements, which retains the record objects as immutable and prohibits deletion or overwrites until the Legal Hold status is cleared.
- Verifies the accuracy and quality of the recording process automatically utilizing (a) advanced storage recording technology and (b) an MD5 checksum that must be received from the source system. The MD5 checksum is stored as a metadata attribute and utilized for post-recording verification.
- Uses a unique combination of attributes to serialize each record object.
- Allows authorized users to access the record objects and metadata with the S3 API for local reproduction or transfer to a format and medium acceptable under the Rule.
- Regenerates an accurate replica of records and metadata (including index attributes) from redundant data, should data be lost or damaged. Alternatively, the *Mirror* functionality, provides continuous synchronization of record objects and associated metadata between source and destination Buckets, resulting in duplicate copies.

Cohasset also correlated the assessed capabilities of MinIO Object Storage, when *Object Lock* mode is set to *Compliance,* to the principles-based electronic records requirements in CFTC Rule 1.31(c)-(d).

Accordingly, Cohasset concludes that MinIO Object Storage, when properly configured and utilized to retain time-based records, meets the five requirements of SEC Rule 17a-4(f) and FINRA Rule 4511(c), which relate to the recording and non-rewriteable, non-erasable storage of records. In addition, the assessed capabilities meet the principles-based electronic records requirements of CFTC Rule 1.31(c)-(d).

# 5 | Overview of Relevant Regulatory Requirements

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

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

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

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

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

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

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

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

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

- A retention period during which the record 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.

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

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 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 and non-rewriteable, non-erasable storage of electronic records and a description of the capabilities of MinIO Object Storage related to each requirement.

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

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

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

## 5.3 Overview of CFTC Rule 1.31(c)-(d) 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 records, 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 and event-time-based 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 MinIO Object Storage in relation to each requirement, see Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*.

# About Cohasset Associates, Inc.

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

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

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

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

***For domestic and international clients, Cohasset:***

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

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

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

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