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-re writable, 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.

Object Storage on the Oracle Cloud Infrastructure (OCI) platform, offers internet-scale, high-performance storage for unstructured data. The Locked Retention Rule feature was designed to meet securities industry requirements for preserving records in a non-re writable, non-erasable format, by protecting each record from being modified, overwritten or deleted until the specified retention period has expired and any associated legal holds have been released.

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

- 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 17 CFR § 1.31(c)-(d), which regulates commodity futures trading.

It is Cohasset’s opinion that Object Storage, when properly configured, meets the five requirements related to the recording and non-re writable, non-erasable storage of electronic records and supports the regulated entity in meeting the remainder of the seventeen electronic records requirements of SEC Rule 17a-4(f). Additionally, the assessed capabilities of Object Storage meet the principles-based requirements of CFTC Rule 1.31(c)-(d) and the requirements defined in the MiFID II Directive and the supplementing Delegated Regulation.
# Table of Contents

Abstract ................................................................................................................................................. 1

Table of Contents ................................................................................................................................. 2

1 | Introduction ....................................................................................................................................... 3
   1.1 Overview of the Regulatory Requirements ............................................................................... 3
   1.2 Purpose and Approach .................................................................................................................. 4
   1.3 Object Storage Overview and Assessment Scope ..................................................................... 5

2 | Assessment of Compliance with SEC Rule 17a-4(f) ......................................................................... 7
   2.1 Non-Rewritable, Non-Erasable Record Format ........................................................................ 7
   2.2 Accurate Recording Process ......................................................................................................... 13
   2.3 Serialize the Original and Duplicate Units of Storage Media .................................................. 15
   2.4 Capacity to Download Indexes and Records .............................................................................. 16
   2.5 Readable Projection or Production of Images for Examination .................................................. 17
   2.6 Reproduction of Images Provided to Regulators ...................................................................... 18
   2.7 Duplicate Copy of the Records Stored Separately .................................................................... 19
   2.8 Organization and Accuracy of Indexes ....................................................................................... 20
   2.9 Availability of Indexes for Examination ..................................................................................... 21
   2.10 Duplicate Copy of the Index Stored Separately ....................................................................... 22
   2.11 Preservation of Indexes ............................................................................................................. 22
   2.12 Audit System .............................................................................................................................. 23
   2.13 Availability of Audit System for Examination ......................................................................... 24
   2.14 Preservation of Audit Results ................................................................................................... 25
   2.15 90-Day Notification and Compliance Representation ............................................................... 26
   2.16 Availability of Information to Access Records and Indexes or Escrow ................................... 26
   2.17 Designated Third Party Requirement ....................................................................................... 28

3 | Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d) ................................................ 29

4 | Summary Assessment of Compliance with MiFID II Durable Medium Requirements for Recordkeeping ................................................................................................................................................ 34

5 | Conclusions ....................................................................................................................................... 39

6 | Overview of Relevant Regulatory Requirements ............................................................................ 41
   6.1 Overview of SEC Rule 17a-4(f) Electronic Records Storage Requirements ............................ 41
   6.2 Overview of FINRA Rule 4511(c) Electronic Records Storage Requirements ........................ 43
   6.3 Overview of CFTC Rule 1.31(c)-(d) Electronic Regulatory Records Requirements ................ 43
   6.4 Overview of MiFID II Durable Medium Requirements for Recordkeeping ............................. 45

About Cohasset Associates, Inc. .............................................................................................................. 47
1 | Introduction

Regulators, world-wide, establish explicit requirements for regulated entities that elect to retain books and records 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 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 6.1, 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.

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, 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 Object Storage. Additionally, refer to Section 6.3, *Overview of CFTC Rule 1.31(c)-(d) Electronic Regulatory Records Requirements*.

1.1.4 **MiFID II Requirements**

On May 20, 1997, the concept of *durable medium* was first introduced in the European Union in the *Distance Selling Directive 97/7/EC* as an alternative to paper as the support or medium for information.

On January 3, 2018, *Directive 2014/65/EU*, Markets in Financial Instruments Directive II (MiFID II), became effective and established a definition of durable medium for recordkeeping. As a supplement to MiFID II, the *Commission Delegated Regulation (EU) 2017/565 (Delegated Regulation)*, requires records to be *retained in a medium that allows the storage of information in a way accessible for future reference by the competent authority* and specifies the recordkeeping conditions that must be met.

Refer to Section 4, *Summary Assessment of Compliance with MiFID II Durable Medium Requirements*, which correlates these MiFID II requirements to the capabilities of Object Storage. Additionally, refer to Section 6.4, *Overview of MiFID II Durable Medium Requirements for Recordkeeping*.

1.2 **Purpose and Approach**

Oracle engaged Cohasset Associates, Inc. (Cohasset) to independently assess the functionality of Object Storage relative to a number of key regulations and prepare a report to help customers determine the suitability of this service in light of their regulatory requirements. 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 CFTC. Additional information about Cohasset is provided in the last section of this report.

Oracle engaged Cohasset to:

- Assess the capabilities of Object Storage, in comparison to the seventeen requirements of SEC Rule 17a-4(f) for the recording, storage and management of electronic records; see Section 2, *Assessment of Compliance with SEC Rule 17a-4(f)*;

---


• Associate the principles-based requirements of CFTC Rule 1.31(c)-(d) to the assessed capabilities of Object Storage; see Section 3, Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d);

• Associate the durable medium requirements of MiFID II and the retention of records requirements in Article 72(1) of the Delegated Regulation, which supplements MiFID II, to the assessed capabilities of Object Storage; see Section 4, Summary Assessment of Compliance with MiFID II Durable Medium Requirements; 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 Object Storage and its capabilities or other Oracle 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 Oracle 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 Object Storage Overview and Assessment Scope

Object Storage on the Oracle Cloud Infrastructure (OCI) platform, offers internet-scale, high-performance storage for any type of unstructured data, including analytic data, large application datasets, logs, images, and videos.

The logical storage architecture of Object Storage is depicted in Figure 1, below.

- **Tenant** – an OCI account within a specified home region (geographical area). Contains identity access management (IAM) resources for the account. **Note:** If an additional region is subscribed to, the tenancy IAM resources will be shared, however they reside in and are managed from the home region only.

- **Namespace** – a single, logical, top-level container for all Buckets and objects.

- **Buckets** – logical containers that store objects.

- **Compartments** – security-related groupings of Buckets. Rules applied to a compartment
determine group access rights (i.e., the actions that may be performed by a group of system users) on Buckets and their objects.

- **Metadata Storage** – multi-tenant Oracle databases that retain meaningful indexes (metadata attributes) regarding the Buckets and record objects stored within the Namespace.

Object Storage offers multiple storage classes to accommodate the lifecycle status of stored data (i.e., hot data to cold data).

Oracle designed the *Locked Retention Rule* feature to store record objects, across all storage classes, in compliance with SEC Rule 17a-4(f) and other similar regulatory requirements. When a *Time-bound Retention Rule* (i.e., one that specifies retention duration) is defined for a Bucket and locked (hereinafter referred to as a *Locked Retention Rule*), integrated controls are applied which prevent the modification, overwrite or premature deletion of the Bucket’s record objects for the designated retention period. Additionally, when litigation or a subpoena requires record objects to be placed on hold, an *Indefinite Retention Rule* can be defined for a Bucket to immutably preserve the Bucket’s record objects for the duration of the hold. Once released, retention controls are returned to any assigned *Locked Retention Rules*.

The scope of this assessment is focused on the compliance-related capabilities of Object Storage, utilized with *Locked Retention Rules*, in the following deployments:

- OCI public cloud offering, including Commercial, Government and Dedicated Regions (i.e., localized geographic areas consisting of one or more Oracle data centers) across all storage classes.
- On premises, via Dedicated Region Cloud@Customer, running on Oracle hardware located in the regulated entity’s data center. *Note: Cloud-at-Customer (Gen 1) is excluded from this assessment.*

Throughout this assessment, the above described operating environments of Object Storage are being assessed.
2 | Assessment of Compliance with SEC Rule 17a-4(f)

This section presents Cohasset’s assessment of the capabilities of Object Storage, for compliance with the seventeen requirements related to recording, storage and management of electronic records, as stipulated in SEC Rule 17a-4(f).

For each of the seventeen 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 Object Storage
- **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 Object Storage, as described in Section 1.3, *Object Storage Overview and Assessment Scope*, relative to each requirement of SEC Rule 17a-4(f).

2.1 Non-Rewritable, 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]."

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, 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 Object Storage, with Locked Retention Rules, meets this SEC requirement to retain records in non-rewriteable, non-erasable format for time-based\(^6\) retention periods and any applied legal hold, 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 Object Storage Capabilities

This section describes the capabilities of Object Storage that directly pertain to this SEC requirement for preserving electronic records as non-rewriteable, non-erasable for the required retention period and any associated legal holds.

2.1.3.1 Overview

- Retention rules are defined at the Bucket level and apply integrated control codes to prevent premature deletion of all record objects contained within that Bucket. Two types of retention rules are available for use:
  1. Time-bound Retention Rules retain record objects for a specified duration of time (i.e., in terms of days, months or years).
  2. Indefinite Retention Rules retain record objects indefinitely, until the Retention Rule is removed from the Bucket. Indefinite Retention Rules can be defined for a Bucket when litigation or a subpoena require the Bucket's record objects to be immutably preserved for the duration of the hold, which may exceed the retention period designated in applied Time-bound Retention Rules.

- Multiple Time-bound and Indefinite Retention Rules can apply to a single Bucket. Indefinite Retention Rules always take precedence, followed by the longest retention associated with any applied Time-bound Retention Rules.

- While Object Storage offers both Compliance and Governance retention modes, only Compliance mode meets the requirements of SEC 17a-4(f).

\(^6\) Time-based retention periods require records to be retained for a specified contiguous period of time from the date and time created and stored.
• Compliance mode is set for a Bucket and its contents when a *Time-bound Retention Rule* is *locked*. A *Locked Retention Rule* applies stringent integrated controls which prevent the modification, overwrite or premature deletion of the Bucket’s record objects and associated metadata for the designated retention period.

• Additionally, once a *Locked Retention Rule* is applied to a Bucket:
  ▪ The assigned retention period cannot be shortened, only extended.
  ▪ The *Locked Retention Rule* cannot be removed from the Bucket.
  ▪ The Bucket cannot be deleted unless it is empty.

**Record Objects, Buckets and Retention Controls**

► Record objects are uploaded to Object Storage either from within the cloud platform or directly from the internet, via multiple interfaces including the Object Storage console, Command Line Interface (CLI), native Object Storage APIs, Amazon S3 Compatibility APIs, and SWIFT APIs.

► A record object within Object Storage is comprised of the following elements:
  
  ● **Content:** The complete content of the unstructured object, such as analytic data, large application datasets, logs, images, and videos.

  ● **Immutable system metadata:** Critical attributes for the record object, such as the object name, prefix, Bucket name, unique eTag (i.e., unique identifier), last modified timestamp (used to compute retention expiration date), user-specified metadata as key value pairs, and MD5 hash value.

  ● **Mutable metadata:** Attributes for the record object, such as storage class tier.

  *Note: Attributes associated with Retention Rules are properties of the Bucket, not the record object.*

► Within a tenant’s Namespace, record objects are stored in logical containers, called Buckets. Buckets are grouped according to security requirements (i.e., user group access rights) into Compartments.

  ● Bucket names must be unique within a Namespace (a maximum of 10,000 Buckets are allowed by default).

  ● Within each Bucket, record objects are stored in a flat storage hierarchy, however, a simulated directory structure (i.e., using a prefix string for object names, including the forward slash “/”) may be used to help organize sets of objects.

► Retention is defined at the Bucket level, via retention rules, which apply to all record objects contained within that Bucket. There are two types of retention rules:

  1. **Time-bound Retention Rules** retain record objects for a specified duration of time. Retention duration is specified in terms of years and days and is added to each record object’s last-modified timestamp to determine its retention expiration date. *Note: retention expiration dates are calculated for each record object during requests for overwrites or deletion; no retention expiration date attribute is stored with the record object.*
Time-bound Retention Rules must be locked (Locked Retention Rules) to assure that stringent Compliance mode retention controls are applied which prevent the modification, overwrite or premature deletion of the Bucket’s record objects and associated metadata for the designated retention period. Only Locked Retention Rules are compliant with the requirements of SEC 17a-4(f).

- A Retention Rule is active immediately, however, there is a default waiting period of 14 days (i.e., scheduled lock wait time) before the lock takes effect, during which time the Retention Rule can be modified and/or deleted from a Bucket. The scheduled lock wait time can be changed, prior to the lock taking effect, from the default value to any future date.

- Once the lock takes effect:
  - The Locked Retention Rule cannot be removed from the Bucket, by any means.
  - The assigned retention period cannot be shortened, only extended.
  - The Bucket cannot be deleted unless it is empty.

*Note: Time-bound Retention Rules that are not locked, operate in Governance Mode and are not compliant with SEC Rule 17a-4(f), since authorized users may modify and/or remove an unlocked Retention Rule from a Bucket at any time.*

2. Indefinite Retention Rules retain record objects indefinitely, until the Retention Rule is removed from the Bucket. Indefinite Retention Rules cannot be locked and therefore, are used for legal holds or other temporary suspension of deletion eligibility. Indefinite Retention Rules cannot be used as a substitute for a properly configured Locked Retention Rule for compliance with the Rule.

- Retention Rules may be applied to both new and existing Buckets, across all storage classes.
  - Retention Rule names are automatically generated by Object Storage and may be modified as necessary.
  - Retention Rule attributes are properties of the Bucket.
  - Up to 100 Locked Retention Rules and Indefinite Retention Rules can apply to a single Bucket. Indefinite Retention Rules always take precedence, followed by the longest retention period of the applied Time-bound Retention Rules. The maximum retention duration that is applied to the Bucket is considered the protection period for all record objects contained within the Bucket.

- When the retention duration of a Locked Retention Rule is extended, the new duration applies to all existing and new record objects stored in the Bucket.

- Record objects stored in a Bucket with an applied Locked Retention Rule:
  - Cannot be moved to another Bucket.
  - May be copied to another Bucket. New record objects created via a copy action are assigned a new last-modified timestamp and will inherit any retention rules associated with the destination Bucket, if any. The original remains unchanged, with the original retention rules applied to it.
• May be assigned to a new storage class. Reassignment of the storage class does not impact retention or immutability controls for the record object.

 A Bucket with an applied Locked Retention Rule:

• May be moved to other Compartments within the Namespace. Moves to other Namespaces are not allowed.
• Cannot be copied, however, individual objects retained in the Bucket may be copied, as described above.

 Record objects that are uploaded via a multi-part upload operation to a Bucket with a Locked Retention Rule are not protected by retention controls until the entire upload operation successfully completes. Should any segment of the multi-part upload fail, an error message is issued and the uploaded fragments are (a) not protected and (b) cannot be retrieved.

2.1.3.2 Legal Holds (Temporary Holds)

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

 Authorized users assign an Indefinite Retention Rule to Buckets which contain record objects subject to the hold. Indefinite Retention Rules take precedence over other time-bound retention rules that are applied to the Bucket.

 While subject to an Indefinite Retention Rule record objects cannot be modified, overwritten or deleted by any means, even if past their retention period.

 The Indefinite Retention Rule can be removed by authorized users when the hold is no longer required. Thereafter, immutability controls for the record object are governed by the time-bound retention rules applied to the Bucket.

2.1.3.3 Deletion

 While deletion is not required by the SEC Rule, record objects are eligible for deletion, when the following conditions are met:

• The retention period applied to the record object (as calculated by adding the Bucket’s longest, time-bound retention duration to the last-modified timestamp for the record object) is in the past, and
• No Indefinite Retention Rules are applied to the record object’s Bucket.

 Deletion of eligible record objects may be initiated in one of the following ways:

• Lifecycle policies can be created to automatically delete eligible record objects according to a regularly scheduled, automated deletion process.
• One or more record objects may be deleted by using the OCI Console, CLI or SDKs.

 Deleting a Bucket with protected record objects is prohibited.

• A Locked Retention Rule applied to a Bucket cannot be removed, which means all record objects in the Bucket must have been eligible for deletion and deleted before the Bucket can be deleted.
2.1.3.4 Clock Management

► To protect against the possibility of premature deletion of record objects that could result from accelerating the system time clock, every Object Storage system clock within an OCI region is configured to synchronize with external time servers, e.g., network time protocol (NTP) clocks. The Object Storage system clock(s) is/are automatically checked against the external time source and resynchronized as required. This constant synchronization prevents, or immediately corrects, inadvertent or intentional administrative modifications to an Object Storage time clock that could result in the premature deletion of record objects.

● Should Object Storage time clocks exceed set thresholds for synchronization, Object Storage stops functioning until the problem is corrected by authorized Oracle administrators.

► The regulated entity does not have access to Object Storage system clocks at any time.

► Timestamps are recorded based on UTC and measured in milliseconds to meet at least one second granularity of time measurement.

2.1.3.5 Security

Oracle publishes a Cloud Security Alliance Consensus Assessment Initiative Questionnaire (CAIQ) that is available for customers to review the security practices to determine the risks associated with the use of these Cloud services. Independent third-party audits of Oracle’s infrastructure, services, and operations are undertaken on a regular basis to verify security, privacy, and compliance controls.

In addition to the stringent retention protection and management controls described above, Object Storage provides the following security capabilities, which support the authenticity and reliability of the record objects.

► Object Storage encrypts objects at rest on the server via 256-bit Advanced Encryption Standard (AES-256). Each object is encrypted with its own data encryption key; the encryption key itself is then encrypted via a master encryption key assigned to the Bucket. By default, Oracle manages master encryption keys.

● Optionally, the regulated entity may elect to encrypt each object using a customer-provided encryption key.

► Hypertext transport-layer encryption (HTTPS) is used to protect data in transit.

► Object Storage supports private access from OCI resources via a Virtual Cloud Network service gateway.

► OCI Identity Access Management (IAM) Policies are required to grant appropriate system, group and user access to the Object Storage environment. OCI offers federated support for any externally implemented IAM SAML 2.0 tool, however, OCI IAM is always responsible for controlling access within the Object Storage environment.

► At no time does the regulated entity have Root access, or access to the storage layer of Object Storage.
2.1.4 Additional Considerations

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

- Applying a Locked Retention Rule with appropriate retention duration, to each Bucket intended to retain regulated record objects. Objects required for compliance with the Rule should be stored in the Bucket only after the waiting period, e.g., 14 day scheduled lock wait time, has lapsed. Care should be taken to ensure that the assigned retention duration for a Bucket reflects the longest retention requirement of all record objects in that Bucket.

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

- Storing record objects requiring event-based retention periods in a separate compliance system, since Object Storage does not currently support event-based retention periods.

- Applying an Indefinite Retention Rule to Buckets that contain record objects subject to preservation for legal matters, government investigations, external audits and other similar circumstances, and removing the Indefinite Retention Rule when the applicable action is completed. Note: An Indefinite Retention Rule is not a substitute for a properly configured Locked Retention Rule.

- Creating IAM policies to ensure appropriate access to the Namespace and its contents.

- Appropriately managing encryption keys, if utilizing customer-provided encryption keys.

- Additionally, the regulated entity is responsible for maintaining their OCI Object Storage account in good standing to ensure that protection of record objects continue until their retention periods have expired and any Indefinite Retention Rule holds have been released.

- If the regulated entity discontinues its use of Object Storage or severs their contractual relationship with Oracle prior to the expiration of the retention period and release of associated holds, the regulated entity must assure that the record objects, associated metadata, and audit trail events are transferred to another compliant storage media prior to the deletion of record objects from Object Storage.

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.

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

---

7 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.
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 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 Object Storage Capabilities

The recording and the post-recording verification processes for Object Storage are described in the following subsections.

#### 2.2.3.1 Recording Process:

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

- During the upload process, Object Storage calculates an MD5 hash value for each object. If the source application transmits an MD5 hash with the record object, Object Storage compares the supplied hash to its calculated hash and either (a) writes the record object to storage and records the MD5 hash value in the metadata services database, if the hash values match or (b) issues an error message and fails the write, if the hash values do not match.

- If no checksum is provided by the source system, Object Storage calculates a hash value upon receipt of the uploaded record object and returns the calculated hash value to the source system as verification of a successful write.

- If a SHA256 hash value is provided by the source system (i.e., via Amazon S3 Compatibility API), Object Storage calculates its own SHA256 value to validate transmission but does not retain the SHA256 value in the Metadata Storage database.

- By default, during the write process record objects are divided into chunks and each chunk is encrypted. A checksum is then calculated for each encrypted chunk and committed to storage with the chunk. Chunk-level checksums are subsequently used for post-recording quality and integrity checks as well as automated record object repair.

- If storage quotas are established for an account and Object Storage determines that insufficient space exists to record the record object, the write process will be blocked.

#### 2.2.3.2 Post-Recording Verification Process:

- During retrieval of a record object, Object Storage recalculates the checksum for each chunk and compares it to the checksum stored with the chunk. If the checksums are not equal, Object Storage repairs or reconstructs the record object from duplicates or erasure-coded segments.
To validate continued data integrity, Object Storage actively scans data at rest to verify that recalculated checksums match stored values. In the event the checksums do not match, Object Storage automatically initiates the repair or reconstruction of the damaged object from duplicates or erasure-coded segments.

Object Storage actively monitors that correct levels of data redundancy are maintained. Should a loss of redundancy occur, Object Storage automatically rebuilds the necessary redundancy.

2.2.4 Additional Considerations

When storing a record object, Cohasset recommends that the source application send a checksum to confirm a successful transmission and write of the record object.

2.3 Serialize the Original and Duplicate Units of Storage Media

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

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

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

2.3.2 Compliance Assessment

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

2.3.3 Object Storage Capabilities

- Object Storage assigns a unique identifier, called an eTag, to each record object and stores it as immutable metadata.
- The last-modified timestamp (storage date and time) is captured and stored with each record object as immutable metadata.
- The combination of the eTag and the last-modified timestamp provide a serialization of 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.

2.4.2 Compliance Assessment

It is Cohasset’s opinion that Object Storage meets 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 Object Storage Capabilities

The following capabilities support the capacity to search and download record objects and indexes (metadata attributes):

- Object Storage deployed in the OCI public cloud, assures that hardware and software capacity allow for ready access to the record objects and indexes (metadata attributes). Further, Object Storage maintains redundant storage media, network, and power to mitigate outages that would otherwise result in unavailability of data. OCI has a Service Level Agreement (SLA) of 99.9% availability for all data in Object Storage.

- The Object Storage console provides the ability to list Buckets that exist within a given Compartment. When an individual Bucket is selected, a list of the objects it contains is displayed in alphabetical order by record object name, along with any user-specified metadata, as key value pairs.
  - Prefixes and/or time-stamps, if utilized as part of the record object naming convention, can be leveraged to filter the list of objects displayed.
  - To view the contents of a record object, it must be downloaded and viewed utilizing client-side tools.

- With APIs and CLI commands, authorized users can (a) list all Buckets or filter the list based on Bucket attributes, (b) list all record objects within a Bucket, or filter the list of objects within a Bucket based on prefixes and/or timestamps, if utilized as part of the record object naming convention, (c) download the list of record objects and associated indexes (metadata attributes), (d) download selected objects for viewing and/or further filtering by client-side tools, and (e) produce the record objects and indexes (metadata attributes).
  - Bucket-level metadata includes Bucket name, creation date, and all applied retention rule(s).
  - Record object metadata includes object name, eTag, and last-modified timestamp. *Note: Calculated retention expiration dates for record objects are not provided by Object Storage as part of Object lists. Instead, the Bucket Retention Rules must be viewed to identify the longest period (i.e., the protection period), which is then used to calculate the retention expiration date for record objects.*

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.
2.4.4 Additional Considerations

The regulated entity is responsible for (a) maintaining its account in good standing, (b) maintaining hardware and software to access Object Storage, (c) maintaining its encryption keys that have been used in addition to the Oracle encryption keys, and (d) assuring that the regulator, self-regulatory organization or designated examining authority receive downloads of the record objects and metadata (index) attributes, in the requested format and medium.

2.5 Readable Projection or Production of Images for Examination

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

This requirement, to display or produce a human-readable view or reproduction of the records, ensures that authorized staff members of the SEC or self-regulatory organizations have immediate and easy access to the requested records for examination. This necessitates having adequate technology to immediately produce the views or reproductions of the requested records in a human-readable format.

2.5.2 Compliance Assessment

Cohasset affirms that Object Storage supports the regulated entity's compliance with this SEC requirement for an easily readable projection of the record objects.

2.5.3 Object Storage Capabilities

- Object Storage encrypts both data at rest and the key used to encrypt the data. Object Storage automatically decrypts the data, as part of the process of rendering the data for use. By default, Oracle maintains the encryption keys for data at rest, however, the regulated entity has the option of managing its own keys.
- See section 2.4.3 for details on the capacity to search for and download record objects and indexes (metadata attributes).
- Once downloaded, local client-side capabilities may be used to render a human-readable projection or print of the record objects.

2.5.4 Additional Considerations

The regulated entity is responsible for (a) maintaining its account in good standing, (b) maintaining its encryption keys that have been used in addition to the Oracle encryption keys, and (c) having hardware and software to view or print the record object.
2.6 Reproduction of Images Provided to Regulators

2.6.1 Compliance Requirement [SEC 17a-4(f)(3)(ii)]

Not knowing in advance whether the SEC, self-regulatory organization or State securities regulator will have ready access to appropriate retrieval and viewing equipment, this requires the regulated entity to immediately produce requested records on paper or in the format and medium stipulated.

Section III. Reproposed Amendments and Discussion, J. Technical Amendments in the October 9, 1998, Federal Register proposed technical amendments to clarify that SROs and State securities regulators need access to facsimile enlargements and downloaded records:

SEC 17a-4(f)(3)(ii): Be ready at all times to provide, and immediately provide, any facsimile enlargement which the staffs of the Commission, any self-regulatory organization of which it is a member, or any State securities regulator having jurisdiction over the member, broker or dealer may request

2.6.2 Compliance Assessment

Cohasset upholds that Object Storage supports the regulated entity in meeting this SEC requirement to provide regulators with reproductions of the record objects.

2.6.3 Object Storage Capabilities

- Object Storage encrypts both data at rest and the key used to encrypt the data. Object Storage automatically decrypts the data, as part of the process of rendering the data for use. By default, Oracle maintains the encryption keys for data at rest, however, the regulated entity has the option of managing its own keys.

- See section 2.4.3 for details on the capacity to search for and download record objects and indexes (metadata attributes).

- Once downloaded, local client-side capabilities may be used to (a) render a human-readable projection, (b) print the record objects, and/or (c) provide downloads of the record objects and index (metadata attributes) in standard format and medium.

2.6.4 Additional Considerations

The regulated entity is responsible for (a) maintaining its account in good standing, (b) maintaining its encryption keys that have been used in addition to the Oracle encryption keys, and (c) assuring that the regulator, self-regulatory organization or designated examining authority receive downloads of the record objects, in the requested format and medium.
2.7 Duplicate Copy of the Records Stored Separately

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

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.

2.7.2 Compliance Assessment

Cohasset asserts that Object Storage meets this SEC requirement for a persistent duplicate copy of the record objects, when the considerations described in Section 2.7.4 are satisfied.

2.7.3 Object Storage Capabilities

- To ensure persistent duplicate copies, record objects are written to Object Storage utilizing either (a) erasure coding or (b) synchronously recording three copies of each record object across multiple fault domains (i.e., separate storage racks and/or storage servers and where available, across multiple data centers).
  - The method of duplicating is dependent upon the capabilities of the OCI region hosting the data as well as the size of each record object.
- The record object is recoverable by either:
  - Regenerating a duplicate of the original from erasure encoded data, or
  - Automatically restoring the record object from a duplicate located in a separate fault domain.
- The erasure coded data and duplicate copies are retained for the full retention period of the record object and any applied legal holds.
- Additionally, a convenience copy of each record object may be obtained by configuring the Object Storage replication feature. Note: Object Storage replication is not compliant with SEC 17a-4(f), due to the inability to set or replicate Locked Retention Rules on replication destination Buckets.

2.7.4 Additional Considerations

For Dedicated Region Cloud@Customer deployments, proper hardware sizing must be performed to ensure appropriate capacity for erasure coding and/or duplicate copies.
2.8 Organization and Accuracy of Indexes

2.8.1 Compliance Requirement [SEC 17a-4(f)(3)(iv)]

The intent of this requirement is to ensure that the electronic records and duplicate copies can be readily searched, identified and retrieved, using an accurate set of indexes or metadata.

2.8.2 Compliance Assessment

Cohasset affirms that Object Storage supports the regulated entity in meeting this SEC requirement to accurately organize and index both the original and duplicate copies.

2.8.3 Object Storage Capabilities

- When record objects are recorded, Object Storage stores the following indexes (metadata attributes) for each record object:
  - **Immutable system metadata:** Critical attributes for the record object, such as the object name, prefix, Bucket name, unique eTag (i.e., unique identifier), last modified timestamp (used to compute retention expiration date), and user-specified metadata as key value pairs.

- **Mutable metadata:** Attributes for the record object, such as storage class tier.

- Bucket-level metadata includes Bucket name, creation date, Y/N flag indicating that Retention Rules are applied, and the actual text of all applied retention rules.

- Within each Bucket, record objects are stored in a flat storage hierarchy, however, a simulated directory structure (i.e., using a prefix string for object names, including the forward slash "/") may be used to help organize and search for sets of objects.

2.8.4 Additional Considerations

The regulated entity is responsible for assigning appropriate Bucket and record object names. Careful planning is required, on the part of the regulated entity, to assign appropriate retention policies to Buckets such that the record objects are retained for the required retention period.

Additionally, the regulated entity is responsible for storing and managing optional key value pairs and any other index or metadata needed to meet the requirements of the SEC Rule. This may include index or metadata retained by the source application.
2.9 Availability of Indexes for Examination

2.9.1 Compliance Requirement [SEC 17a-4(f)(3)(iv)(A)]

This requirement recognizes that indexes are necessary for finding and retrieving records. It is meant to ensure accessibility to the index information by the SEC or self-regulatory organizations, which includes its availability for examination. Additionally, given the prevalence of technology and standards for sharing electronic data, the regulator may request electronic copies of index data and may specify the format and medium for delivery.

2.9.2 Compliance Assessment

Cohasset asserts that Object Storage can retrieve and download the record object indexes (metadata attributes) that it maintains, which supports the regulated entity in meeting this SEC requirement.

2.9.3 Object Storage Capabilities

► Object Storage deployed in the OCI public cloud, assures that hardware and software capacity allows for ready access to the record objects and indexes (metadata attributes). Further, Object Storage maintains redundant storage media, network, and power to mitigate outages that would otherwise result in unavailability of data. OCI has a Service Level Agreement (SLA) of 99.9% availability for all data in Object Storage.

► The Object Storage console provides the ability to list Buckets that exist within a given Compartment. When an individual Bucket is selected, a list of the objects it contains is displayed in alphabetical order by record object name, along with any user-specified metadata as key value pairs.

• Prefixes and/or time-stamps, if utilized as part of the record object naming convention, can be leveraged to filter the list of objects displayed.

• To view the contents of a record object, it must be downloaded and viewed utilizing client-side tools.

► With APIs and CLI commands, authorized users can (a) list all Buckets or filter the list based on Bucket attributes, (b) list all record objects within a Bucket, or filter the list of objects within a Bucket based on prefixes and/or timestamps, if utilized as part of the record object naming convention, (c) download the list of record objects and associated indexes (metadata attributes), (d) download selected objects for viewing and/or further filtering by client-side tools, and (e) produce the record objects and indexes (metadata attributes) in a format and on a medium acceptable under the Rule.

► Record object indexes (metadata attributes) are retained for the lifespan of the associated record object.

► Bucket-level indexes (metadata attributes) are retained for the lifespan of the associated Bucket.

► See Section 2.8.3 for available indexes (metadata attributes).

2.9.4 Additional Considerations

The regulated entity is responsible for (a) maintaining its account in good standing, (b) maintaining hardware and software to access Object Storage, (c) maintaining its encryption keys that have been used in addition to the
Oracle encryption keys, and (d) assuring that the regulator, self-regulatory organization or designated examining authority receive downloads of indexes (metadata attributes) in the requested format and medium.

### 2.10 Duplicate Copy of the Index Stored Separately

#### 2.10.1 Compliance Requirement [SEC 17a-4(f)(3)(iv)(B)]

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

Although this requirement may appear to be somewhat duplicative of SEC Rule 17a-4(f)(3)(iii) addressed in Section 2.7 of this report, the two requirements are complementary. The earlier requirement pertains to information comprising the record content, whereas this requirement pertains to the index metadata associated with the record.

#### 2.10.2 Compliance Assessment

It is Cohasset's preliminary opinion that Object Storage meets this SEC requirement for a persistent duplicate copy of the index (metadata attributes) that it maintains.

#### 2.10.3 Object Storage Capabilities

- To ensure persistent duplicate copies:
  - **Object-level indexes** (metadata attributes) are written to Metadata Storage databases, utilizing both replication and RAID technologies in the recording process.
  - **Bucket-level indexes** (metadata attributes), including actual text of applied Retention Rules, are written to Object Storage utilizing either (a) erasure coding, or (b) synchronously recording three copies of each index across multiple fault domains (i.e., separate storage racks and/or storage servers.)

#### 2.10.4 Additional Considerations

There are no additional considerations related to this requirement for the indexes (metadata attributes) stored in Object Storage.

### 2.11 Preservation of Indexes

#### 2.11.1 Compliance Requirement [SEC 17a-4(f)(3)(iv)(C)]

This requirement ensures that both the original and duplicate index is preserved for the same period of time as the indexed record (and the duplicate of the record). Accordingly, this ensures the records are findable as a result of the index being retained as long as the associated record.
2.11.2 Compliance Assessment

It is Cohasset’s opinion that Object Storage meets this SEC requirement for the preservation of indexes (metadata attributes).

2.11.3 Object Storage Capabilities

- Copies of object-level indexes (metadata attributes) are retained for the same time period as the associated record object.
- Copies of Bucket-level indexes (metadata attributes) are retained for the life of the Bucket.
- See Section 2.8.3 for available indexes (immutable and mutable metadata attributes).
- See Section 2.10.3 for duplication mechanisms for indexes (metadata attributes).

2.11.4 Additional Considerations

There are no additional considerations related to this requirement for the metadata (index) attributes stored in Object Storage.

2.12 Audit System

2.12.1 Compliance Requirement [SEC 17a-4(f)(3)(v)]

Meeting this provision requires an audit system which provides accountability (e.g., when, by whom and what action was taken) for both initially inputting and tracking changes made to the original and duplicate records and associated retention metadata.

2.12.2 Compliance Assessment

When both the OCI Audit service and Logging service features are enabled, Cohasset asserts that Object Storage meets this SEC requirement for an audit system.

2.12.3 Object Storage Capabilities

- Object Storage offers two types of audit logging features to capture lifecycle events:
  - Bucket-level logs are captured in the OCI Audit service.
  - Object-level logs are captured in the Logging service.
- Audit logging entries include, but are not limited to, the user and timestamp for the following actions taken:
  - Uploading a record object, including the Namespace, Compartment and Bucket where the record object is stored.
  - Deleting eligible record objects and associated metadata, including failed attempts to delete ineligible record objects.
  - Creating a Retention Rule for a specific Bucket, including the name of the rule, the type (i.e., Indefinite or Time-bound), and the associated retention duration.

SEC 17a-4(f)(3)(v): The member, broker, or dealer must have in place an audit system providing for accountability regarding inputting of records required to be maintained and preserved pursuant to §§ 240.17a-3 and 240.17a-4 to electronic storage media and inputting of any changes made to every original and duplicate record maintained and preserved thereby.
• Modifying a Retention Rule, including the previous and new values (i.e., extending the retention duration).
• Deleting a Retention Rule (i.e., deleting an Indefinite Retention Rule).

2.12.4 Additional Considerations

The regulated entity is responsible for (a) enabling audit logging for their OCI account, (b) retaining audit log activity as described in Section 2.14, Preservation of Audit Results and (c) capturing an audit trail of transactions initiated by the source system, for object-level activities that are not currently captured by Object Storage, if required for regulatory compliance.

2.13 Availability of Audit System for Examination

2.13.1 Compliance Requirement [SEC 17a-4(f)(3)(v)(A)]

The intent of this requirement is to ensure that the audit trail is available for examination, upon request, by the SEC or self-regulatory organizations.

2.13.2 Compliance Assessment

When the OCI Audit service and Logging service features are enabled, Cohasset affirms that Object Storage supports efforts to meet this SEC requirement to make the audit system available to the regulated entity for submission to the SEC or self-regulatory organization.

2.13.3 Object Storage Capabilities

• The OCI Audit service and Logging service retain logs in an audit index for a period of time and makes them available via the OCI Explore Log Groups user interface.

• During the availability period, authorized users can search for all, or a filtered subset, of log events and (a) display a summary list of log events on the OCI screen, (b) download the log events and (c) utilize client-side tools to produce the audit log events in a format acceptable under the Rule.

• Search criteria includes:
  • Field name or text.
  • Time of log entry.
  • Log Group name.

2.13.4 Additional Considerations

The regulated entity is responsible for (a) maintaining its account in good standing, (b) conducting searches to locate requested audit trail data, during the availability period, (c) printing, downloading or otherwise producing audit trail data in the requested format and medium, and (d) providing the produced audit trail data to the regulator, self-regulatory organization or designated examining authority.
2.14 Preservation of Audit Results


It is the intent of this requirement to ensure that the audit trail information is preserved for the same period of time as the associated records.

SEC 17a-4(f)(3)(v)(B): The audit results must be preserved for the time required for the audited records

2.14.2 Compliance Assessment

When OCI Audit service and Logging service features are enabled, Cohasset asserts its opinion that Object Storage supports efforts to meet this SEC requirement to retain the audit results for the same time period as the audited records.

2.14.3 Object Storage Capabilities

- The OCI Audit service and Logging service can be configured to retain logs in an audit index for a limited period of time and make them accessible via the OCI Explore Log Groups user interface.
  - Bucket-level audit logs can be retained for a maximum of 365 days.
  - Object-level audit logs can be retained for a maximum of 180 days.
- Authorized users must export the audit trail activities from the Audit service and Logging service indexes to another solution for longer retention.
- OCI Service Connectors may be used to automatically export audit log data from both the Audit service and Logging service indexes, for long term storage in either:
  - A client-side security information event management tool utilized to retain the audit trail events for the required retention period.
  - An Object Storage Bucket, that is configured with an appropriate Retention Rule. Note: If this option is selected, log files are retained as separate record objects, external to the audit logging services. Therefore, these files are not viewable using the OCI Explore Log Groups user interface. Instead, these separately stored logs (i.e., record objects) must be downloaded to a client-side system to view content or produce in a format and on a medium acceptable under the Rule

2.14.4 Additional Considerations

The regulated entity is responsible for (a) configuring an appropriate availability period for Bucket-level and object-level audit logs, (b) exporting audit trail events from the OCI Audit service and Logging service indexes, during the availability period, (c) capturing the audit trail for object-level activities initiated by source systems that are not currently captured by Object Storage, if required for regulatory compliance, and (d) storing the audit trail for the required retention period.
2.15 90-Day Notification and Compliance Representation

2.15.1 Compliance Requirement [SEC 17a-4(f)(2)(i)]

This requirement is the responsibility of the regulated entity, which must notify its designated examining authority at least 90 days prior to employing electronic storage media, other than optical disk technology. The regulated entity must provide its representation (or one from the storage medium vendor or other third party, with the appropriate expertise) that the selected storage media meets the conditions set forth in SEC Rule 17a-4(f)(2)(ii).

2.15.2 Compliance Assessment

The member, broker, or dealer is responsible for filing the 90-day notification letter described in SEC Rule 17a-4(f)(2)(i).

2.15.3 Object Storage Capabilities

- The regulated entity is responsible for notifying its designated examining authority at least 90 days prior to employing electronic storage media, other than optical disk technology, as required by this SEC Rule.
- This Assessment Report and other documentation may be provided to the regulated entity for preparation of its notification letter.

2.15.4 Additional Considerations

There are no additional considerations related to this requirement.

2.16 Availability of Information to Access Records and Indexes or Escrow

2.16.1 Compliance Requirement [SEC 17a-4(f)(3)(vi)]

This requirement is intended to provide the SEC or self-regulatory organizations with sufficient information to access records and indexes, independent of any support from the regulated entity. This requirement, along with SEC Rule 17a-4(f)(3)(vii), described in Section 2.17, Designated Third Party Requirement, are designed to provide the SEC and self-regulatory organizations with access to the indexes and records, should the regulated entity not cooperate or not be available.

2.16.2 Compliance Assessment

Cohasset asserts that Object Storage meets this SEC requirement to maintain current information needed to access the electronic records and associated indexes (metadata attributes).
2.16.3 Object Storage Capabilities

- For deployments on the OCI public cloud offering, Object Storage retains record objects and index (metadata attributes) in a cloud environment, under the control of Oracle, rather than on the premises of the regulated entity.
  - Oracle maintains the necessary infrastructure for authorized users to access the record objects and indexes (metadata attributes).
- For Dedicated Region Cloud@Customer deployments, Oracle hardware is located on the premises of the regulated entity, and as such, Oracle is dependent upon the regulated entity to maintain network access to the Oracle hardware.
- For both types of deployments, administration of the solution is shared by Oracle and the regulated entity’s administrators.
- Oracle maintains and makes publicly available information needed to access the electronic record objects and associated index (metadata attributes) and offers technical support, as needed.
- Oracle maintains the encryption keys it uses to encrypt data at rest.
- Should the regulated entity cease operation, Oracle maintains the information necessary for authorized users to access the record objects and indexes (metadata attributes), with the exception of encryption keys managed by the regulated entity.
- Should the regulated entity cease paying for Object Storage, Oracle will retain the regulated entity’s information, as per the terms and conditions stated in its contract with the regulated entity.

2.16.4 Additional Considerations

- The regulated entity is responsible for placing in escrow or otherwise making available its encryption keys that have been used, in addition to the Oracle encryption keys.
- In the event that Oracle no longer provides access to the Object Storage cloud-based system, Oracle will provide a method for customers to retrieve and transfer their data, as documented in the Oracle Terms of Service and/or the customer’s specific contract terms.
2.17 Designated Third Party Requirement

2.17.1 Compliance Requirement

[SEC 17a-4(f)(3)(vi)]

This requirement is the joint responsibility of the regulated entity and the third party it employs to adhere to this requirement. It is intended to provide the SEC, self-regulatory organizations, and State securities regulators with access to records and indexes, independent of any support from the regulated entity, should the regulated entity not cooperate, be in receivership or no longer exist. The July 15, 1993, Federal Register, issued proposed amendments to the Rule; Section H. Proposed Amendments and Discussion specified:

The proposed conditions also are designed to provide access to information preserved in optical disks [or other compliant electronic solutions] when the broker-dealer is no longer operational, when the broker-dealer refuses to cooperate with the investigative efforts of the Commission or the SROs, or when the optical disk [or other compliant electronic solutions] has not been properly indexed as to its entire contents.

2.17.2 Compliance Assessment

The member, broker, or dealer is responsible for entering into an agreement for Designated Third Party services, as required in SEC Rule 17a-4(f)(3)(vii).

2.17.3 Object Storage Capabilities

Obtaining Designated Third-Party services is the responsibility of the broker-dealer.

2.17.4 Additional Considerations

The regulated entity is responsible for placing in escrow or otherwise making available its encryption keys that have been used, in addition to the Oracle encryption key.

SEC 17a-4(f)(3)(vii): For every member, broker, or dealer exclusively using electronic storage media for some or all of its record preservation under this section, at least one third party ("the undersigned"), who has access to and the ability to download information from the member's, broker's, or dealer's electronic storage media to any acceptable medium under this section, must file with the designated examining authority for the member, broker, or dealer the following undertakings with respect to such records:

The undersigned hereby undertakes to furnish promptly to the U.S. Securities and Exchange Commission ("Commission"), its designees or representatives, any self-regulatory organization of which it is a member, or any State securities regulator having jurisdiction over the member, broker or dealer, upon reasonable request, such information as deemed necessary by the staffs of the Commission, any self-regulatory organization of which it is a member, or any State securities regulator having jurisdiction over the member, broker or dealer to download information kept on the member's, broker's or dealer's electronic storage media to any medium acceptable under § 240.17a-4. Furthermore, the undersigned hereby undertakes to take reasonable steps to provide access to information contained on the member's, broker's or dealer's electronic storage media, including, as appropriate, arrangements for the downloading of any record required to be maintained and preserved by the member, broker or dealer pursuant to §§ 240.17a-3 and 240.17a-4 in a format acceptable to the staffs of the Commission, any self-regulatory organization of which it is a member, or any State securities regulator having jurisdiction over the member, broker or dealer. Such arrangements will provide specifically that in the event of a failure on the part of a member, broker or dealer to download the record into a readable format and after reasonable notice to the broker or dealer, upon being provided with the appropriate electronic storage medium, the undersigned will undertake to do so, as the staffs of the Commission, any self-regulatory organization of which it is a member, or any State securities regulator having jurisdiction over the member, broker or dealer may request.
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 Object Storage, as described in Section 1.3, 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 CFTC Rule may be achieved by meeting the SEC requirements.

When comparing the capabilities of 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:
  1. Any data necessary to access, search, or display any such books and records; and
  2. 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 Object Storage with Locked Retention Rules (Compliance Mode), which is a highly restrictive configuration that assures 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 Object Storage with Locked Retention Rules (Compliance Mode) 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 Object Storage with Governance Mode (Unlocked Time-bound Retention Rules), 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 applied retention period. This less restrictive Governance Mode provides flexibility to remove or shorten retention periods, 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 Object Storage 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

<table>
<thead>
<tr>
<th>Compliance Assessment Relative to CFTC 1.31(c)-(d)</th>
<th>SEC 17a-4(f) Requirements Listed in the Referenced Sections</th>
</tr>
</thead>
</table>
| (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: | Section 2.1 Non-Rewritable, Non-Erasable Record Format  
Preserve the records exclusively in a non-rewriteable, non-erasable format |
| (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. | Section 2.2 Accurate Recording Process  
Verify automatically the quality and accuracy of the storage media recording process |
| (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: | 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 |
| (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; | 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. |
| It is Cohasset’s opinion that the capabilities of Object Storage, utilized with Retention Rules, 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: | Section 2.8 Organization and Accuracy of Indexes  
Organize and index accurately all information maintained on both original and any duplicate storage media |
| (i) Any data necessary to access, search, or display any such books and records; and | Section 2.11 Preservation of Indexes  
Original and duplicate indexes must be preserved for the time required for the indexed records |
| (ii) All data produced and stored electronically describing how and when such books and records were created, formatted, or modified. [emphasis added] | Section 2.12 Audit System  
The member, broker, or dealer must have in place an audit system providing for accountability regarding inputting of records required to be maintained and preserved pursuant to §§ 240.17a-3 and 240.17a-4 to electronic storage media and inputting of any changes made to every original and duplicate record maintained and preserved thereby |
| It is Cohasset’s opinion that Object Storage retains indexes (metadata attributes) as an integral part of either the (a) record object; or (b) Bucket. Object-level attributes are subject to the same retention protections as the associated record objects and Bucket-level attributes are subject to the same retention protections as the associated Bucket. See Sections 2.8 and 2.11 for Object Storage capabilities related to the authenticity and reliability of indexes. Object Storage creates an audit trail of actions taken and supports two methods of storing the audit trail for the same time period as the record object. See Sections 2.12 through 2.14 for capabilities related to the authenticity and reliability of the audit trail. To satisfy this requirement for other essential data that is not retained in Object Storage (such as separate indices), the regulated entity must retain this other data in a compliant manner. | Section 2.13 Availability of Audit System for Examination  
At all times, a member, broker, or dealer must be able to have the results of such audit system available for examination by the staffs of the Commission and the self-regulatory organizations of which the broker or dealer is a member |
| The audit results must be preserved for the time required for the audited records | Section 2.14 Preservation of Audit Results  
The audit results must be preserved for the time required for the audited records |

---

**Cohasset Associates**

Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d) • 31
### CFTC 1.31(c)-(d) Requirement

<table>
<thead>
<tr>
<th>Description</th>
<th>Compliance Assessment Relative to CFTC 1.31(c)-(d)</th>
<th>SEC 17a-4(f) Requirements Listed in the Referenced Sections</th>
</tr>
</thead>
<tbody>
<tr>
<td>(ii) Systems that ensure the records entity is able to produce electronic</td>
<td>It is Cohasset's opinion that the Object Storage capabilities described in the following sections meet the</td>
<td>Section 2.7 Duplicate Copy of the Records Stored Separately</td>
</tr>
<tr>
<td>regulatory records 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</td>
<td>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.</td>
<td>Store separately from the original, a duplicate copy of the record stored on any medium acceptable under §240.17a-4 for the time required</td>
</tr>
<tr>
<td></td>
<td>Object Storage deployed in the OCI public cloud, assures that hardware and software capacity allow for ready access to the record objects and indexes (metadata attributes). Further, Object Storage maintains redundant storage media, network, and power to mitigate outages that would otherwise result in unavailability of data. OCI has a Service Level Agreement (SLA) of 99.9% availability for all data in Object Storage. Sections 2.7 and 2.10 explain that Object Storage maintains persistent duplicate copies of both record objects and indexes (metadata attributes) allowing for recovery should the primary source be compromised. In Section 2.14.3 Cohasset explains that OCI Audit service and Logging service data is retained and readily accessible for a period of time. During this availability period, it may be exported to an Object Storage Bucket or a client-side security information event management tool and retained for the same period as the associated record objects. To satisfy this requirement for other essential data that is not retained in Object Storage (such as separate indices), the regulated entity must retain this other data in a compliant manner.</td>
<td>Section 2.10 Duplicate Copy of the Index Stored Separately Each index must be duplicated and the duplicate copies must be stored separately from the original copy of the index Section 2.14 Preservation of Audit Results The audit results must be preserved for the time required for the audited records</td>
</tr>
<tr>
<td>(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.</td>
<td>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).</td>
<td>N/A</td>
</tr>
</tbody>
</table>

---

8 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.
<table>
<thead>
<tr>
<th>CFTC 1.31(c)-(d) Requirement</th>
<th>Compliance Assessment Relative to CFTC 1.31(c)-(d)</th>
<th>SEC 17a-4(f) Requirements Listed in the Referenced Sections</th>
</tr>
</thead>
</table>
| (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: | It is Cohasset's opinion that the capabilities described in the following sections support the regulated entity's efforts to comply with the CFTC requirements for inspection and production of regulatory records stored electronically. Specifically, it is Cohasset's opinion that: | 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 |
| (1) Inspection. All regulatory records shall be open to inspection by any representative of the Commission or the United States Department of Justice. | ● Sections 2.4, 2.5, and 2.6, pertain to the inspection and production of record objects. | Section 2.5 Readable Projection or Production of Images for Examination
At all times have available, for examination by the staffs of the Commission and self-regulatory organizations of which it is a member, facilities for immediate, easily readable projection or production of micrographic media or electronic storage media images and for producing easily readable images |
| (2) Production of paper regulatory records. *** | ● Sections 2.4, 2.9 and 2.11 pertain to the inspection and production of indexes. | Section 2.6 Reproduction of Images Provided to Regulators
Be ready at all times to provide, and immediately provide, any facsimile enlargement which the staffs of the Commission, any self-regulatory organization of which it is a member, or any State securities regulator having jurisdiction over the member, broker or dealer may request |
| (3) Production of electronic regulatory records. | ● Section 2.13 pertains to the inspection and production of the audit trail. | Section 2.9 Availability of Indexes for Examination
At all times, a member, broker, or dealer must be able to have such indexes available for examination by the staffs of the Commission and the self-regulatory organizations of which the broker or dealer is a member |
| (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. | Further, as noted in the Additional Considerations in Sections 2.4, 2.6, 2.9, and 2.13, the regulated entity is obligated to produce and provide the records, index and audit trail (respectively) in the form and medium requested. If the regulator requests additional data related to how and when the record objects were created, formatted, or modified, the regulated entity will need to provide this information from appropriate source systems. | Section 2.11 Preservation of Indexes
Original and duplicate indexes must be preserved for the time required for the indexed 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. | | Section 2.13 Availability of Audit System for Examination
At all times, a member, broker, or dealer must be able to have the results of such audit system available for examination by the staffs of the Commission and the self-regulatory organizations of which the broker or dealer is a member |
| (4) Production of original regulatory records. *** | | |
4 | Summary Assessment of Compliance with MiFID II Durable Medium Requirements for Recordkeeping

The objective of this section is to document Cohasset’s assessment of the capabilities of Object Storage, as described in Section 1.3, Object Storage Overview and Assessment Scope, in comparison to the MiFID II requirements.

The concept of durable medium, as an alternative to paper, was first introduced in the European Union on May 20, 1997, in the Distance Selling Directive 97/7/EC. Since 1997, many EU regulations have adopted the concept of durable medium. The definition of durable medium recognizes the evolution of technology and the interests of both customers and service providers to have the ability to transition from paper to electronic storage.

The MiFID II definition of durable medium focuses on storability, accessibility, retention and immutable reproduction:

(62) ‘durable medium’ means any instrument which:
(a) enables a client to store information addressed personally to that client in a way accessible for future reference and for a period of time adequate for the purposes of the information; and
(b) allows the unchanged reproduction of the information stored [emphasis added]

MiFID II was further supplemented by Commission Delegated Regulation (EU) 2017/565. Article 72(1) specifies recordkeeping practices for the retention of records:

1. The records shall be retained in a medium that allows the storage of information in a way accessible for future reference by the competent authority, and in such a form and manner that the following conditions are met:
(a) the competent authority is able to access them readily and to reconstitute each key stage of the processing of each transaction;
(b) it is possible for any corrections or other amendments, and the contents of the records prior to such corrections or amendments, to be easily ascertained;
(c) it is not possible for the records otherwise to be manipulated or altered;
(d) it allows IT or any other efficient exploitation when the analysis of the data cannot be easily carried out due to the volume and the nature of the data; and
(e) the firm’s arrangements comply with the record keeping requirements irrespective of the technology used.

Both the EU definition of durable medium and the above paragraph (e) recognize the technology evolution and defines requirements or conditions for regulated entities that retain records electronically. The approach is consistent with the SEC, which also set forth standards that the electronic storage media must satisfy to be considered acceptable.

The focus of this assessment pertains to Object Storage, with Locked Retention Rules (Compliance Mode), which are highly restrictive and assure that the storage solution applies controls to (a) protect the immutability of the record content and certain metadata and (b) prevent deletion over the applied retention period.

In this section, Cohasset correlates the capabilities of Object Storage, with Locked Retention Rules (Compliance Mode), to the durable medium definition in MiFID II and retention of records requirements in Article 72(1) of the Delegated Regulation. Additionally, Cohasset contends that Object Storage used in Governance Mode (Unlocked Time-bound Retention Rules) meets the MiFID II and EU durable medium requirements, when the regulated entity applies appropriate procedural controls to oversee operations that may allow content to be changed or deleted.
prior to expiration of the retention period. This less restrictive *Governance Mode* provides flexibility to shorten retention periods, which may be beneficial for compliance with privacy and data protection requirements.

For each of the four requirements, which are highlighted in the light blue rows, the following table summarizes the results of Cohasset's analysis:

- The two left-hand columns list key requirements specified in (a) the definition of *durable medium* in MiFID II and (b) the retention of records in the *Delegated Regulation*, which supplements MiFID II, respectively. The focal element for each row is underlined for clarity.
- The right-hand column provides Cohasset's compliance assessment and an analysis of capabilities of Object Storage, relative to these requirements.
### Regulatory excerpts that are pertinent to each of the four specific requirements

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirement #1: Store record for the required retention period</td>
<td></td>
</tr>
</tbody>
</table>

(62) ‘durable medium’ means any instrument which:

(a) enables a client to store information addressed personally to that client in a way accessible for future reference and for a period of time adequate for the purposes of the information ***** [emphasis added] |

(1) The records shall be retained in a medium that allows the storage of information in a way accessible for future reference by the competent authority, and in such a form and manner that the following conditions are met: ***** [emphasis added] |

While this requirement pertains to the client of the regulated entity, the regulated entity itself would have a similar need to store the record for the required retention period. It is Cohasset’s opinion that Object Storage has features that apply a retention period to a record object and its metadata, via Retention Rules that are applied at the Bucket-level, as described in Section 2.1 Non-Rewritable, Non-Erasable Record Format. The resulting integrated control codes:

- Prohibit modification and overwrites for the protection period of the record object.
- Prohibit deletion, through any mechanism, until the assigned retention period expires and any legal holds (Indefinite Retention Rules) are removed.

Further, Object Storage assures the accurate recording (storage) of the record content and associated metadata, as explained in Section 2.2 Accurate Recording Process. The quality and accuracy of the recording process is verified: (a) during the initial recording of the record object, (b) using post-recording verification during read-back, and, (c) by conducting periodic consistency and integrity checking.
<table>
<thead>
<tr>
<th>Regulatory excerpts that are pertinent to each of the four specific requirements</th>
<th>Compliance Assessment and Analysis of Object Storage Relative to the MiFID II Directive and the Supplementing Delegated Regulation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Requirement #2: Assure immutable record content</strong></td>
<td>It is Cohasset's opinion that the features of Object Storage, with Locked Retention Rules, achieve the non-rewriteable, non-erasable storage requirements necessary to assure that record content is unchangeable. See Section 2.1 Non-Writeable, Non-Erasable Record Format for additional information. If the regulated entity corrects or amends a record object in the source system, it must store each rendition as a new record object. The features for assuring a non-rewriteable, non-erasable format assure that the original record is not modified. Further, Object Storage calculates and retains chunk-level checksums during the recording process and subsequently uses it for post-recording quality and integrity checks and for automated record object repair, as described in Section 2.2 Accurate Recording Process.</td>
</tr>
<tr>
<td>(62) ‘durable medium’ means any instrument which: (a) enables a client to store information addressed personally to that client in a way accessible for future reference and for a period of time adequate for the purposes of the information (b) allows the unchanged reproduction of the information stored [emphasis added]</td>
<td>1. The records shall be retained in a medium that allows the storage of information in a way accessible for future reference by the competent authority, and in such a form and manner that the following conditions are met: (b) it is possible for any corrections or other amendments, and the contents of the records prior to such corrections or amendments, to be easily ascertained; (c) it is not possible for the records otherwise to be manipulated or altered; (d) it allows IT or any other efficient exploitation when the analysis of the data cannot be easily carried out due to the volume and the nature of the data; and (e) the competent authority is able to access them readily and to reconstitute each key stage of the processing of each transaction; (f) it is possible for any corrections or other amendments, and the contents of the records prior to such corrections or amendments, to be easily ascertained; (g) it is not possible for the records otherwise to be manipulated or altered; (h) it allows IT or any other efficient exploitation when the analysis of the data cannot be easily carried out due to the volume and the nature of the data; and (i) the competent authority is able to access them readily and to reconstitute each key stage of the processing of each transaction.</td>
</tr>
<tr>
<td><strong>Requirement #3: Provide access to and reproduce the stored records</strong></td>
<td>Cohasset asserts that Object Storage provides the following methods of retrieving records: 1. Direct searches via the Object Storage console 2. APIs 3. CLI commands The selected record objects and associated metadata may be downloaded, and local capabilities may be used to view, filter, or produce in a format and on an acceptable medium. See Section 2.4 Capacity to Download Indexes and Records for additional information. Further, Object Storage ensures that records are readily available by ensuring persistent duplicate copies exist. Record objects are written to Object Storage utilizing either (a) erasure coding or (b) synchronously recording three copies of each record object across multiple fault domains (i.e., separate storage racks and/or storage servers). The</td>
</tr>
<tr>
<td>(62) ‘durable medium’ means any instrument which: (a) enables a client to store information addressed personally to that client in a way accessible for future reference and for a period of time adequate for the purposes of the information (b) allows the unchanged reproduction of the information stored [emphasis added]</td>
<td>1. The records shall be retained in a medium that allows the storage of information in a way accessible for future reference by the competent authority, and in such a form and manner that the following conditions are met: (b) it is possible for any corrections or other amendments, and the contents of the records prior to such corrections or amendments, to be easily ascertained; (c) it is not possible for the records otherwise to be manipulated or altered; (d) it allows IT or any other efficient exploitation when the analysis of the data cannot be easily carried out due to the volume and the nature of the data; and (e) the competent authority is able to access them readily and to reconstitute each key stage of the processing of each transaction; (f) it is possible for any corrections or other amendments, and the contents of the records prior to such corrections or amendments, to be easily ascertained; (g) it is not possible for the records otherwise to be manipulated or altered; (h) it allows IT or any other efficient exploitation when the analysis of the data cannot be easily carried out due to the volume and the nature of the data; and (i) the competent authority is able to access them readily and to reconstitute each key stage of the processing of each transaction.</td>
</tr>
<tr>
<td>Regulatory excerpts that are pertinent to each of the four specific requirements</td>
<td>Compliance Assessment and Analysis of Object Storage Relative to the MiFID II Directive and the Supplementing Delegated Regulation</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Directive 2014/65/EU (MiFID II)</strong> Article 4(1)(62)</td>
<td><strong>Commission Delegated Regulation (EU) 2017/565, Article 72(1), which supplements MiFID II</strong></td>
</tr>
<tr>
<td></td>
<td>method of duplication is dependent upon the capabilities of the OCI region hosting the data as well as the size of each record object. See <a href="#">Section 2.5 Duplicate Copy of the Records Stored Separately</a> for additional information.</td>
</tr>
</tbody>
</table>

**Requirement #4: Provide access to and reproduce the stored records**

N/A

1. The records shall be retained in a medium that allows the storage of information in a way accessible for future reference by the competent authority, and in such a form and manner that the following conditions are met:

   *****

   (e) the firm’s arrangements comply with the record keeping requirements irrespective of the technology used. *****

   [emphasis added]

Cohasset asserts that Object Storage provides the following methods of retrieving records:

1. Direct searches via the Object Storage console
2. APIs
3. CLI commands

The selected record objects and associated metadata may be downloaded, and local capabilities may be used to view, filter or produce in a format and on an acceptable medium. See [Section 2.4 Capacity to Download Indexes and Records](#) for additional information.

As may be required, the regulated entity may transfer records to other media or migrate record objects to new file formats, in advance of technological obsolescence.
5 | Conclusions

Cohasset assessed the capabilities of Object Storage, with Locked Retention Rules, in comparison to the seventeen requirements related to the recording, storage and management of electronic records, as set forth in SEC Rule 17a-4(f) and its associated Interpretive Releases. (See Section 1.3, Object Storage Overview and Assessment Scope.)

Cohasset determined that Object Storage, when properly configured, as outlined throughout Section 2 of this Assessment Report and in accordance with the publicly available Oracle Cloud Infrastructure documentation, has the following capabilities, which meet the regulatory requirements:

▶ Retaining the record objects in a non-rewriteable, non-erasable format, by applying integrated control codes that prevent modifying, overwriting or deleting a record object for the applied retention period.
  ● Time-bound Retention Rules are applied to an Object Storage Bucket and locked, resulting in the protection of all record objects retained within the Bucket.
  ● Indefinite Retention Rules are applied to an Object Storage Bucket when litigation or a subpoena requires record objects to be placed on hold, resulting in the indefinite protection of all record objects retained within the Bucket.

▶ Verifying the accuracy and quality of the recording process through checksums and Object Storage validation processes, in addition to the inherent capabilities of advanced magnetic storage technology.

▶ Uniquely serializing each record object with an immutable unique identifier (eTag) and last-modified timestamp.

▶ Retaining immutable metadata, such as the record object last-modified timestamp and unique identifier for the full retention period of the record object.

▶ Retaining the full text of all Locked Retention Rules applied to a Bucket for the lifespan of the Bucket.

▶ Regenerating an accurate replica of the record object and indexes (metadata attributes) from a persistent duplicate copy or erasure coded segment, should an error occur in the source record object or an availability problem be encountered.

▶ Providing capacity and tools to (a) list all Buckets or filter the list based on Bucket attributes, (b) list all record objects within a Bucket, or filter the list of objects within a Bucket based on prefixes and/or time-stamps, if utilized as part of the record object naming convention, (c) download the list of record objects and associated indexes (metadata attributes), (d) download selected objects for viewing and/or further filtering by client-side tools, and (e) produce the record objects and indexes (metadata attributes) in a format and on a medium acceptable under the Rule.
Additionally, Object Storage supports the regulated entity’s compliance with audit trail requirements. Audit trail entries must be exported from OCI Audit service and Logging service, during the period of time they are available, and may be stored in an Object Storage Bucket or another tool for the required retention period.

Cohasset also correlated the assessed capabilities of Object Storage, with Locked Retention Rules, to the:

- Principles-based technology requirements of CFTC Rule 1.31(c)-(d),
- Durable medium definition in MiFID II, and retention of records requirements in Article 72(1) of the Delegated Regulation, which supplements MiFID II.

Accordingly, Cohasset concludes that Object Storage, when properly configured and utilized to retain time-based records, meets the five electronic storage-related requirements and meets or supports the regulated entity in meeting the remainder of the seventeen requirements of SEC Rule 17a-4(f). In addition, these capabilities meet the principles-based electronic records requirements of CFTC Rule 1.31(c)-(d) and the durable medium requirements of MiFID II.
6 | **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.

### 6.1 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.


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 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.

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.

---

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 each SEC electronic records storage requirement and a description of the capabilities of Object Storage related to each requirement.

### 6.2 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.*

### 6.3 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 Object Storage in relation to each requirement, see Section 3, Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d).
Overview of MiFID II Durable Medium Requirements for Recordkeeping

Markets in Financial Instruments Directive II (MiFID II), approved by the European Parliament as Directive 2014/65/EU, became effective January 3, 2018. Specifically, Article 4(1)(62) of MiFID II defines durable medium as:

(62) ‘durable medium’ means any instrument which:
(a) enables a client to store information addressed personally to that client in a way accessible for future reference and for a period of time adequate for the purposes of the information; and
(b) allows the unchanged reproduction of the information stored [emphasis added]

The concept of durable medium was first introduced on 20 May 1997 in the Distance Selling Directive 97/7/EC as an alternative to paper as the support or medium for information. Since 1997, various European Union (EU) regulatory provisions require that a firm must provide certain information to a client in writing, either on paper or in another durable medium. Examples include, but not limited to:


Further, with the implementation of the revised MiFID II, investment firms must arrange for records to be kept of all services, activities and transactions. The key recordkeeping provisions are in Article 16, Organisational requirements, paragraphs 6 and 7:

6. An investment firm shall arrange for records to be kept of all services, activities and transactions undertaken by it which shall be sufficient to enable the competent authority to fulfil its supervisory tasks and to perform the enforcement actions under this Directive, Regulation (EU) No 600/2014, Directive 2014/57/EU and Regulation (EU) No 596/2014, and in particular to ascertain that the investment firm has complied with all obligations including those with respect to clients or potential clients and to the integrity of the market.
7. Records shall include the recording of telephone conversations or electronic communications relating to, at least, transactions concluded when dealing on own account and the provision of client order services that relate to the reception, transmission and execution of client orders.

Such telephone conversations and electronic communications shall also include those that are intended to result in transactions concluded when dealing on own account or in the provision of client order services that relate to the reception, transmission and execution of client orders, even if those conversations or communications do not result in the conclusion of such transactions or in the provision of client order services.

For those purposes, an investment firm shall take all reasonable steps to record relevant telephone conversations and electronic communications, made with, sent from or received by equipment provided by the investment firm to an
employee or contractor or the use of which by an employee or contractor has been accepted or permitted by the investment firm.

Orders may be placed by clients through other channels, however such communications must be made in a durable medium such as mails, faxes, emails or documentation of client orders made at meetings. In particular, the content of relevant face-to-face conversations with a client may be recorded by using written minutes or notes. Such orders shall be considered equivalent to orders received by telephone.

The records kept in accordance with this paragraph shall be provided to the client involved upon request and shall be kept for a period of five years and, where requested by the competent authority, for a period of up to seven years.

Article 16(6) allowed the Commission to make delegated legislation, resulting in the issuance of Commission Delegated Regulation (EU) 2017/565.

The Delegated Regulation, supplementing MiFID II, defines record keeping and recording requirements, in Section 8, Record-keeping, Article 72, Retention of records, paragraph 1, which specifies:

1. The records shall be retained in a medium that allows the storage of information in a way accessible for future reference by the competent authority, and in such a form and manner that the following conditions are met:
   (a) the competent authority is able to access them readily and to reconstitute each key stage of the processing of each transaction;
   (b) it is possible for any corrections or other amendments, and the contents of the records prior to such corrections or amendments, to be easily ascertained;
   (c) it is not possible for the records otherwise to be manipulated or altered;
   (d) it allows IT or any other efficient exploitation when the analysis of the data cannot be easily carried out due to the volume and the nature of the data; and
   (e) the firm’s arrangements comply with the record keeping requirements irrespective of the technology used.

See Section 4, Summary Assessment of Compliance with MiFID II Durable Medium Requirements for Recordkeeping, for a summary assessment of the capabilities of Object Storage in relation to requirements for (a) durable medium in MiFID II and (b) retention of records in the Delegated Regulation, which supplements MiFID II.
About Cohasset Associates, Inc.

Cohasset Associates, Inc. ([www.cohasset.com](http://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.

**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.

©2021 Cohasset Associates, Inc.

This Assessment Report and the information contained in it are copyrighted and are the sole property of Cohasset Associates, Inc. Selective references to the information and text of this Assessment Report are welcome, provided such references have appropriate attributions and citations. Permission is granted for in-office reproduction so long as the contents are not edited and the look and feel of the reproduction is retained.