

## Oracle® Object Storage

### COMPLIANCE ASSESSMENT

SEC 17a-4(f), SEC 18a-6(e), FINRA 4511(c), CFTC 1.31(c)-(d)  
and the MiFID II Delegated Regulation (72)(1)

#### Abstract

Object Storage on the Oracle® Cloud Infrastructure (OCI) platform, offers secure, high-performance storage for any type of digital content in its native format. OCI Object Storage is ideal for modern applications that require scale and flexibility. The *Retention Rule* feature, offered as part of Object Storage, was designed to meet securities industry requirements for preserving records in a non-rewriteable, non-erasable format.

In this report, Cohasset Associates, Inc. (Cohasset) assesses the functionality of Object Storage (see Section 1.3, *Object Storage Overview and Assessment Scope*) relative to the electronic records requirements, specified by multiple regulatory bodies, as follows:

- Securities and Exchange Commission (SEC) in 17 CFR § 240.17a-4(f)(2);
- SEC in 17 CFR § 240.18a-6(e)(2);
- Financial Industry Regulatory Authority (FINRA) in 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); and
- the European Parliament and the Council of the European Union in Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing MiFID II (the MiFID II Delegated Regulation), Article 72(1).

It is Cohasset's opinion that Object Storage, with the *Retention Rule* feature, has functionality that meets the requirements for electronic records set forth in the above Rules.

#### COHASSET'S INDUSTRY INSIGHT AND EXPERIENCE

Core to our practice is the delivery of records management and information governance professional consulting services, and education and training. Cohasset's expert consulting services support regulated organizations, including those in financial services. Cohasset serves both domestic and multi-national clients, aligning information lifecycle controls to their organizations' business priorities, facilitating regulatory compliance and risk mitigation, while generating quantifiable business efficiency.

Cohasset assesses a range of electronic recordkeeping systems, each designed to meet the requirements of the Securities and Exchange Commission Rules 17a-4(f)(2) and 18a-6(e)(2) for record audit-trail and non-rewriteable, non-erasable record formats, considering the SEC 2001, 2003 and 2019 interpretations. For the non-rewriteable, non-erasable record, these interpretations authorize the use of erasable storage, conditioned on integrated software or hardware control codes, to prevent overwriting, erasing, or otherwise altering the records, during the applied retention period.

---

## Table of Contents

<b>Abstract</b> .....	<b>1</b>
<b>Table of Contents</b> .....	<b>2</b>
<b>1 • Introduction</b> .....	<b>3</b>
1.1 Overview of the Regulatory Requirements .....	3
1.2 Purpose and Approach .....	4
1.3 Object Storage Overview and Assessment Scope.....	5
<b>2 • Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e)</b> .....	<b>7</b>
2.1 Record and Audit-Trail .....	7
2.2 Non-Rewriteable, Non-Erasable Record Format .....	8
2.3 Record Storage Verification .....	15
2.4 Capacity to Download and Transfer Records and Location Information .....	16
2.5 Record Redundancy .....	18
2.6 Facilities to Produce Records for Examination .....	19
2.7 Provide Records to Regulators.....	20
2.8 Audit System .....	21
2.9 Information to Access and Locate Records.....	23
2.10 Designated Executive Officer or Designated Third Party Requirement.....	24
<b>3 • Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)</b> .....	<b>26</b>
<b>4 • Summary Assessment of Compliance with MiFID II Delegated Regulation(72)(1)</b> .....	<b>29</b>
<b>5 • Conclusions</b> .....	<b>32</b>
<b>Appendix A • Overview of Relevant Electronic Records Requirements</b> .....	<b>34</b>
A.1 Overview of SEC Rules 17a-4(f) and 18a-6(e) <i>Electronic Recordkeeping System</i> Requirements.....	34
A.2 Overview of FINRA Rule 4511(c) <i>Electronic Recordkeeping System</i> Requirements.....	36
A.3 Overview of CFTC Rule 1.31(c)-(d) <i>Electronic Regulatory Records</i> Requirements .....	37
A.4 Overview of the <i>Medium and Retention of Records</i> Requirements of MiFID II .....	38
<b>Appendix B • Cloud Provider Undertaking</b> .....	<b>40</b>
B.1 Compliance Requirement.....	40
B.2 Oracle Undertaking Process.....	40
B.3 Additional Considerations .....	41
<b>About Cohasset Associates, Inc.</b> .....	<b>42</b>

## 1 • Introduction

*Regulators, worldwide, establish explicit requirements for certain regulated entities that elect to electronically retain books and records. Given the prevalence of electronic books and records, these requirements apply to most broker-dealers, commodity futures trading firms and similarly regulated organizations.*

*This Introduction summarizes the regulatory environment pertaining to this assessment and the purpose and approach for Cohasset's assessment. It also provides an overview of Oracle Object Storage and the assessment scope.*

### 1.1 Overview of the Regulatory Requirements

#### 1.1.1 SEC Rules 17a-4(f) and 18a-6(e) Requirements

In 17 CFR §§ 240.17a-3 and 240.17a-4 for the securities broker-dealer industry and 17 CFR §§ 240.18a-5 and 240.18a-6 for nonbank SBS entities<sup>1</sup>, the SEC stipulates recordkeeping requirements, including retention periods.

Effective January 3, 2023, the U.S. Securities and Exchange Commission (SEC) promulgated amendments to 17 CFR § 240.17a-4 (SEC Rule 17a-4) and 17 CFR § 240.18a-6 (SEC Rule 18a-6), which define explicit requirements for electronic storage systems.

*The Securities and Exchange Commission ("Commission") is adopting amendments to the recordkeeping rules applicable to broker-dealers, security-based swap dealers, and major security-based swap participants. The amendments modify requirements regarding the maintenance and preservation of electronic records\*\*\*<sup>2</sup> [emphasis added]*

For additional information, refer to Section 2, *Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e)*, and Appendix A.1, *Overview of SEC Rules 17a-4(f) and 18a-6(e) Electronic Recordkeeping System Requirements*.

#### 1.1.2 FINRA Rule 4511(c) Requirements

Financial Industry Regulatory Authority (FINRA) rules regulate member brokerage firms and exchange markets. These rules were amended to address security-based swaps (SBS).<sup>3</sup>

FINRA Rule 4511(c) explicitly defers to the requirements of SEC Rule 17a-4, for 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. [emphasis added]*

---

<sup>1</sup> Throughout this report, 'nonbank SBS entity' refers to security-based swap dealers (SBSD) and major security-based swap participants (MSBSP) that are not also registered as a broker-dealer without a prudential regulator.

<sup>2</sup> Electronic Recordkeeping Requirements for Broker-Dealers, Security-Based Swap Dealers, and Major Security-Based Swap Participants, Exchange Act Release No. 96034 (Oct. 12, 2022) 87 FR 66412 (Nov. 3, 2022) (2022 Electronic Recordkeeping System Requirements Adopting Release).

<sup>3</sup> FINRA, Regulatory Notice 22-03 (January 20, 2022), FINRA Adopts Amendments to Clarify the Application of FINRA Rules to Security-Based Swaps.

### 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.

For additional information, refer to Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*, and Appendix A.3, *Overview of CFTC Rule 1.31(c)-(d) Electronic Regulatory Records Requirements*.

### 1.1.4 MiFID II Delegated Regulation(72)(1) Requirements

On January 3, 2018, *Directive 2014/65/EU*<sup>4</sup>, Markets in Financial Instruments Directive II (MiFID II), became effective and established a definition of durable medium for recordkeeping to enable the client to store and access its information. As a supplement to MiFID II, the *Commission Delegated Regulation (EU) 2017/565*<sup>5</sup> (the *MiFID II Delegated Regulation*), Article 72(1), 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.

For additional information, refer to Section 4, *Summary Assessment of Compliance with the MiFID II Delegated Regulation(72)(1)*, and Appendix A.4, *Overview of the Medium and Retention of Records Requirements of MiFID II*.

## 1.2 Purpose and Approach

To obtain an independent and objective assessment of the compliance capabilities of Object Storage for preserving required electronic records, Oracle engaged Cohasset Associates, Inc. (Cohasset). As a specialized consulting firm, Cohasset has more than fifty 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 functionality of Object Storage, in comparison to the electronic recordkeeping system requirements of SEC Rules 17a-4(f)(2) and 18a-6(e)(2) and describe features that support the regulated entity in its compliance with SEC Rules 17a-4(f)(3) and 18a-6(e)(3); see Section 2, *Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e)*;
- Address FINRA Rule 4511(c), given FINRA explicitly defers to the requirements of SEC Rule 17a-4; see Section 2, *Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e)*;
- Associate the principles-based requirements of CFTC Rule 1.31(c)-(d) with the assessed functionality of Object Storage; see Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*;

---

<sup>4</sup> *Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments.*

<sup>5</sup> *Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment regulated entities and defined terms for the purposes of that Directive.*

- Associate the requirements of Article 72(1) of the MiFID II Delegated Regulation with the assessed functionality of Object Storage; see Section 4, *Summary Assessment of Compliance with the MiFID II Delegated Regulation(72)(1)*; and
- Prepare this Compliance Assessment Report, enumerating the assessment results.

In addition to applying the information in this Compliance Assessment Report, regulated entities must ensure that the combination of its policies, procedures and regulatory submissions, in conjunction with the functionality of implemented electronic recordkeeping systems, 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 functionality or other Oracle products or services. The information utilized by Cohasset to conduct this assessment consisted of: (a) oral discussions, (b) product demonstrations, (c) system documentation, (d) user and system administrator guides, and (e) 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

### 1.3.1 Object Storage Overview

[Object Storage](#), on the Oracle Cloud Infrastructure (OCI) platform, offers internet-scale, secure, high-performance storage for any type of digital content, including analytics, large application datasets, logs, images, and videos. Content is stored in its native format.

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

- ▶ **Tenant** – an OCI account within a specified home region (localized 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.
- ▶ **Buckets** – logical containers that store records<sup>6</sup>.

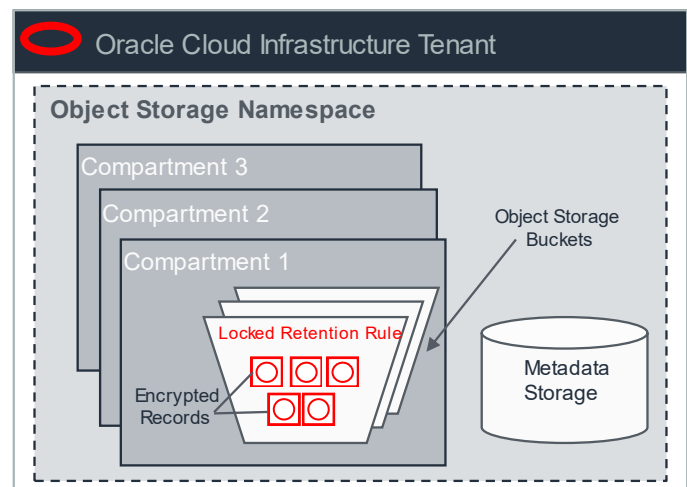


Figure 1: Logical Storage Architecture

<sup>6</sup> The SEC use the phrase *books and records* to describe information that must be retained for regulatory compliance. Cohasset typically uses the term *record* (versus object or data) to recognize that the content is required for regulatory compliance.

- ▶ **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 records.
- ▶ **Metadata Storage** – multi-tenant Oracle databases that retain meaningful metadata attributes regarding the Buckets and records.

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

Oracle designed the *Retention Rule* feature to store required records, 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 records for the designated retention period. Additionally, when litigation or a subpoena requires records to be placed on hold, an *Indefinite Retention Rule* can be defined for a Bucket to immutably preserve the Bucket's records for the duration of the hold. Once released, retention controls are returned to any assigned *Locked Retention Rules*.

### 1.3.2 Assessment Scope

The scope of this assessment is focused specifically on the compliance-related capabilities of Object Storage, utilized with *Locked Retention Rules*.

**NOTE:**

- ▶ Oracle Storage also offers a less-restrictive **unlocked Retention Rule** that provides flexibility for administrators to remove or shorten retention periods, which may be beneficial for compliance with privacy and other data protection requirements. However, for compliance with SEC Rules, in this report, Cohasset assesses the more stringent controls provided with *Locked Retention Rules*.

The following deployments are within the scope of this assessment:

- ▶ OCI public cloud offering, including Commercial, Government and Dedicated Regions (i.e., localized geographic areas consisting of one or more Oracle Cloud 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 Rules 17a-4(f) and 18a-6(e)

This section presents Cohasset's assessment of the functionality of Oracle Object Storage, for compliance with the electronic recordkeeping system requirements promulgated in SEC Rules 17a-4(f)(2) and 18a-6(e)(2), as well as describes how the solution supports the regulated entity in meeting the requirements of SEC Rules 17a-4(f)(3) and 18a-6(e)(3).

For each compliance requirement described in this section, this assessment is organized as follows:

- **Compliance Requirement** – Excerpt of relevant regulatory requirement in SEC Rules 17a-4(f) and 18a-6(e) and Cohasset's interpretation of the specific requirement
  - ◆ Both SEC Rules 17a-4(f) and 18a-6(e) are addressed in this section, since the electronic recordkeeping system requirements (principles, controls and testable outcomes) are the same, though the Rules specify their respective regulations and regulators and include semantic differences.
- **Compliance Assessment** – Summary statement assessing compliance of Object Storage
- **Object Storage Capabilities** – Description of assessed functionality
- **Additional Considerations** – Additional clarification related to meeting the specific requirement

The following sections document Cohasset's assessment of the capabilities of Object Storage, as described in Section 1.3, *Object Storage Overview and Assessment Scope*, relative to the enumerated requirements of SEC Rules 17a-4(f) and 18a-6(e).

### 2.1 Record and Audit-Tail

#### 2.1.1 Compliance Requirement

This regulatory requirement, adopted with the 2022 Rule amendments, allows regulated entities to use a combination of electronic recordkeeping systems, with each system meeting either (a) the record and audit-trail requirement, as described in this section or (b) the non-rewriteable, non-erasable record format requirement, as explained in Section 2.2, *Non-Rewriteable, Non-Erasable Record Format*.

This record and audit-trail requirement is designed to permit use of the regulated entities' business-purpose recordkeeping systems to achieve the required outcome without specifying any particular technology solution.

#### SEC 17a-4(f)(2)(i)(A) and 18a-6(e)(2)(i)(A):

Preserve a record for the duration of its applicable retention period in a manner that maintains a complete time-stamped audit-trail that includes:

- ( 1) All modifications to and deletions of the record or any part thereof;
- ( 2) The date and time of actions that create, modify, or delete the record;
- ( 3) If applicable, the identity of the individual creating, modifying, or deleting the record; and
- ( 4) Any other information needed to maintain an audit-trail of the record in a way that maintains security, signatures, and data to ensure the authenticity and reliability of the record and will permit re-creation of the original record if it is modified or deleted

The SEC clarifies that this requirement to retain the record and its complete time-stamped audit-trail promotes the authenticity and reliability of the records by requiring the electronic recordkeeping system to achieve the testable outcome of reproducing the original record, even if it is modified or deleted during the required retention period, without prescribing how the system meets this requirement.

*[L]ike the existing WORM requirement, [the audit-trail requirement] sets forth a specific and testable outcome that the electronic recordkeeping system must achieve: the ability to access and produce modified or deleted records in their original form.*<sup>7</sup> [emphasis added]

For clarity, the record and audit-trail requirement applies only to the final records required by regulation.

*[T]he audit-trail requirement applies to the final records required pursuant to the rules, rather than to drafts or iterations of records that would not otherwise be required to be maintained and preserved under Rules 17a-3 and 17a-4 or Rules 18a-5 and 18a-6.*<sup>8</sup> [emphasis added]

## 2.1.2 Compliance Assessment

In this report, Cohasset has not assessed Object Storage in comparison to this requirement of the SEC Rules.

For enhanced control, a business-purpose recordkeeping system may store records and complete time-stamped audit-trails on Object Storage, with the features and controls described in Sections 2.2 through 2.9 of this report.

Reminder: This requirement is an alternative to the non-rewriteable, non-erasable record format requirement (i.e., write-once, read-many or WORM requirement), which is assessed in Section 2.2.

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

### 2.2.1 Compliance Requirement

This regulatory requirement was first adopted in 1997. In the 2022 Rule amendments, regulated entities are allowed

to use a combination of electronic recordkeeping systems, to comply with each system meeting either (a) the non-rewriteable, non-erasable record format requirement described in this section or (b) the complete time-stamped record audit-trail requirement described in Section 2.1, *Record and Audit-Trail*.

The SEC further clarifies that the previously issued interpretations are extant. Therefore, records must be preserved in a non-rewriteable, non-erasable format that prevents overwriting, erasing, or otherwise altering records during the required retention period, which may be accomplished by any combination of hardware and software integrated controls.

*The 2003 interpretation clarified that the WORM requirement does not mandate the use of optical disks and, therefore, a broker-dealer can use "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 2019 interpretation further refined the 2003 interpretation. In particular, it noted that the 2003 interpretation described a process of integrated software and hardware codes and clarified that "a software solution that prevents the*

#### SEC 17a-4(f)(2)(i)(B) and 18a-6(e)(2)(i)(B):

Preserve the records exclusively in a non-rewriteable, non-erasable format

<sup>7</sup> 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.

<sup>8</sup> 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66418.



*overwriting, erasing, or otherwise altering of a record during its required retention period would meet the requirements of the rule.”*

\*\*\*\*\*

*In 2001, the Commission issued guidance that Rule 17a-4(f) was consistent with the ESIGN Act. The final amendments to Rule 17a-4(f) do not alter the rule in a way that would change this guidance.<sup>9</sup> [emphasis added]*

Moreover, records must be preserved beyond established retention periods when certain circumstances occur, such as a subpoena or legal hold:

*[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 retention periods specified in Commission rules.<sup>10</sup> [emphasis added]*

## 2.2.2 Compliance Assessment

It is Cohasset’s opinion that the functionality of Object Storage, with *Locked Retention Rules*, meets this SEC requirement to retain records in non-rewriteable, non-erasable format for the applied time-based<sup>11</sup> retention periods and legal holds, when (a) properly configured, as described in Section 2.2.3, and (b) the considerations described in Section 2.2.4 are satisfied.

**Reminder:** This requirement is an alternative to the complete time-stamped audit-trail requirement, which is addressed in Section 2.1.

## 2.2.3 Object Storage Capabilities

This section describes the functionality of Object Storage that directly pertains to this SEC requirement to preserve electronic books and records in a non-rewriteable, non-erasable format, for the required retention period and any applied legal holds.

### 2.2.3.1 Overview

- ▶ Retention rules are defined at the Bucket level and apply integrated control codes to prevent premature deletion of all records contained within that Bucket. Two types of retention rules are available for use:
  1. *Time-bound Retention Rules* retain records for a specified duration of time (i.e., in terms of days, months or years).
  2. *Indefinite Retention Rules* retain records 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 records to be immutably preserved for the duration of the hold, which may exceed the retention period designated in applied *Time-bound Retention Rules*.

---

<sup>9</sup> 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66419.

<sup>10</sup> Electronic Storage of Broker-Dealer Records, Exchange Act Release No. 47806 (May 7, 2003), 68 FR 25283, (May 12, 2003) (2003 Interpretative Release).

<sup>11</sup> Time-based retention periods require records to be retained for a fixed contiguous period of time from the creation or storage timestamp.

- ▶ 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*.
- ▶ A *Locked Retention Rule* is set for a Bucket and its contents when a *Time-bound Retention Rule* is locked.
- ▶ The following table summarizes the stringent integrated controls that are applied to records by *Locked Retention Rules*.

	<b>Locked Retention Rule – highly-restrictive integrated retention controls</b>
Protecting record content and immutable metadata	<ul style="list-style-type: none"> <li>● By design, the contents of a record and associated system metadata are protected against modification and overwrite for the duration of the retention period assigned to the Bucket.</li> </ul>
Restricting changes to <i>Locked Retention Rule</i> controls	<ul style="list-style-type: none"> <li>● The assigned retention period cannot be reduced, only extended.</li> <li>● The <i>Locked Retention Rule</i> cannot be downgraded to <i>unlocked</i> and cannot be removed from the Bucket.</li> </ul>
Restricting deletion of Buckets and records	<ul style="list-style-type: none"> <li>● The Bucket cannot be deleted unless it is empty.</li> <li>● Deletion of each record and its associated immutable metadata are <u>prohibited</u> before the assigned retention period has expired.</li> </ul>

### 2.2.3.2 Bucket and Identity and Access Management (IAM) Configuration

- ▶ Within a tenant’s Namespace, records are stored in logical containers, called Buckets. Buckets are grouped according to security requirements (i.e., user group access rights) into Compartments.
  - Within each Bucket, records 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 records.
  - Bucket names must be unique within a Namespace (a maximum of 10,000 Buckets are allowed by default).
- ▶ The following table describes Bucket and IAM configurations required for the *Retention Rule* feature.

	<b>Bucket and IAM Configurations related to the <i>Retention Rule</i> feature</b>
<b>Retention Rule feature</b>	<p>Retention is defined at the Bucket level, via retention rules, which apply to all records contained within that Bucket.</p> <p>There are two types of retention rules:</p> <ul style="list-style-type: none"> <li>● <b><i>Time-bound Retention Rules</i></b> retain records for a specified duration of time. Retention duration is specified in terms of years and days and is added to each record’s last-modified timestamp to determine its retention expiration date. <i>Note: retention expiration dates are calculated for each record during requests for overwrites or deletion; no retention expiration date attribute is stored with the record.</i> <ul style="list-style-type: none"> <li>▪ <i>Time-bound Retention Rules</i> must be <u>locked</u> (<b><i>Locked Retention Rules</i></b>) to assure that stringent retention controls are applied which prevent the modification, overwrite or premature deletion of the Bucket’s records and associated metadata for the designated retention period.</li> <li>▪ 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.</li> </ul> </li> </ul>

	Bucket and IAM Configurations related to the <i>Retention Rule</i> feature
	<ul style="list-style-type: none"> <li>▪ Once the lock takes effect:                             <ul style="list-style-type: none"> <li>• The <i>Locked Retention Rule</i> cannot be removed from the Bucket, by any means.</li> <li>• The assigned retention period cannot be reduced, only extended.</li> <li>• The Bucket cannot be deleted unless it is empty.</li> </ul> </li> <li>• <b><i>Indefinite Retention Rules</i></b> retain records indefinitely, until the retention rule is removed from the Bucket. <i>Indefinite Retention Rules</i> cannot be locked and therefore, are used for legal holds or other <u>temporary suspension of deletion eligibility</u>. <i>Indefinite Retention Rules</i> cannot be used as a substitute for a properly configured <i>Locked Retention Rule</i> for compliance with the Rules.</li> <li>• Retention rules may be applied to both new and existing Buckets, across all storage classes.                             <ul style="list-style-type: none"> <li>○ Retention Rule names are automatically generated by Object Storage and may be modified as necessary.</li> <li>○ Retention rule attributes are properties of the Bucket.</li> <li>○ Up to 100 <i>Locked Retention Rules</i> and <i>Indefinite Retention Rules</i> can apply to a single Bucket. <i>Indefinite Retention Rules</i> always take precedence, followed by the longest retention period of the applied <i>Time-bound Retention Rules</i>. The maximum retention duration that is applied to the Bucket is considered the <i>protection period</i> for all records contained within the Bucket</li> </ul> </li> </ul>
<b>Versioning</b>	<ul style="list-style-type: none"> <li>• Versioning must be disabled or suspended on a Bucket that will be used with retention rules. Once an active retention rule is applied to a Bucket, versioning cannot be enabled or reactivated.</li> </ul>
<b>IAM Policies</b>	<ul style="list-style-type: none"> <li>• IAM Policies define a set of permissions that grant access to actions and resources in Oracle Cloud Infrastructure, including Object Storage namespaces, Buckets, and associated objects. Care must be taken to ensure the appropriate restrictions are placed on IAM Policies that govern retention rule operations.</li> </ul>

### 2.2.3.3 Records and Retention Controls

- ▶ Records 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 within Object Storage is comprised of the following elements:
  - **Immutable Content:** The complete content of the record, such as analytic data, large application datasets, logs, images, and videos.
  - **Immutable system metadata:** Critical attributes for the record, such as the record 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, such as storage class tier.

*Note: Attributes associated with retention rules are properties of the Bucket, not the record.*

- ▶ The following table describes the retention controls applied during record creation/storage.

	<b>Locked Retention Rules – highly-restrictive integrated retention controls</b>
<b>Version management</b>	<ul style="list-style-type: none"> <li>Versioning is not allowed for objects protected by a <i>Locked Retention Rule</i>.</li> </ul>
<b>Modifying record content or overwriting</b>	<ul style="list-style-type: none"> <li>By design, the contents of a record and associated system metadata are protected against modification and overwrite for the duration of the retention period assigned to the Bucket.</li> </ul>
<b>Modifying or removing retention controls</b>	<ul style="list-style-type: none"> <li>The <i>Locked Retention Rule</i> cannot be removed from the Bucket, by any means.</li> <li>The assigned retention period cannot be reduced, only extended. When the retention duration of a <i>Locked Retention Rule</i> is extended, the new duration applies to <b>all existing and new</b> records stored in the Bucket.</li> </ul>
<b>Deleting Buckets and records</b>	<ul style="list-style-type: none"> <li>The Bucket cannot be deleted unless it is empty.</li> <li>Deletion of each record and its associated immutable metadata are <u>prohibited</u> before the applied retention period has expired.</li> </ul>
<b>Copying records and Buckets</b>	<ul style="list-style-type: none"> <li>Records may be copied to another Bucket. New records 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.</li> <li>Buckets cannot be copied, however, individual records retained in the Bucket may be copied, as described above.</li> </ul>
<b>Moving records and Buckets</b>	<ul style="list-style-type: none"> <li>Records cannot be moved to another Bucket.</li> <li>Buckets may be moved to other Compartments within the Namespace. Moves to other Namespaces are not allowed.</li> </ul>
<b>Storage Class</b>	<ul style="list-style-type: none"> <li>Records may be assigned to a new storage class. Reassignment of the storage class does not impact retention or immutability controls for the record.</li> </ul>

- ▶ Records 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.

### 2.2.3.4 Legal Holds (Temporary Holds)

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

The following table describes *Indefinite Retention Rules* that are used to apply legal holds.

	<b>Indefinite Retention Rules</b>
<b>Applying and removing legal holds</b>	<ul style="list-style-type: none"> <li>Authorized users assign an <i>Indefinite Retention Rule</i> to Buckets which contain records subject to the hold. <i>Indefinite Retention Rules</i> take precedence over other time-bound retention rules that are applied to the Bucket.</li> <li>The <i>Indefinite Retention Rule</i> can be removed by authorized users when the hold is no longer required. Thereafter, immutability controls for the record are governed by the time-bound retention rules applied to the Bucket.</li> </ul>
<b>Legal hold Protections</b>	<ul style="list-style-type: none"> <li>While subject to an <i>Indefinite Retention Rule</i>, records cannot be modified, overwritten or deleted by any means, even if past their retention period.</li> </ul>

### 2.2.3.5 Deletion Controls

- ▶ While deletion is **not** required by the SEC Rule, records are *eligible for deletion*, when the following conditions are met:
  - The retention period applied to the record (as calculated by adding the Bucket’s longest, time-bound retention duration to the last-modified timestamp for the record) is in the past, and
  - No *Indefinite Retention Rules* are applied to the record’s Bucket.
- ▶ The following table summarizes actions taken to delete records:

	<b>Locked Retention Rules – highly-restrictive integrated retention controls</b>
<b>Manually Deleting records</b>	<ul style="list-style-type: none"> <li>● One or more eligible records may be deleted by using the OCI Console, CLI or SDKs.</li> </ul>
<b>Using a Lifecycle Policy for deletion</b>	<ul style="list-style-type: none"> <li>● Lifecycle policies can be created to automatically delete eligible records according to a regularly scheduled, automated deletion process.</li> </ul>
<b>Deleting Buckets</b>	<ul style="list-style-type: none"> <li>● Deleting a Bucket with protected records is prohibited. A <i>Locked Retention Rule</i> applied to a Bucket cannot be removed, which means all records in the Bucket must have been <i>eligible for deletion</i> and deleted before the Bucket can be deleted.</li> </ul>

### 2.2.3.6 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 records.

- ▶ Object Storage encrypts records at rest on the server via 256-bit Advanced Encryption Standard (AES-256). Each record 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 record 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.

### 2.2.3.7 Clock Management

- ▶ To protect against the possibility of premature deletion of records 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 records.
  - 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.

### 2.2.4 Additional Considerations

In addition, for this non-rewriteable, non-erasable record format requirement, the regulated entity is responsible for:

- ▶ Applying a *Locked Retention Rule* with appropriate retention duration, to each Bucket intended to retain required records. Records required for compliance with the Rules 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 records in that Bucket.
- ▶ Ensuring all records required to be retained for compliance with the SEC Rules 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 records requiring event-based<sup>12</sup> retention periods in a separate compliant system, since Object Storage does not currently support event-based retention periods.
- ▶ Applying an *Indefinite Retention Rule* to Buckets that contain records 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.*
- ▶ Appropriately managing encryption keys, if utilizing customer-provided encryption keys.

Additionally, the regulated entity is responsible for: (a) maintaining its OCI Object Storage account in good standing and paying for appropriate services to allow records to be retained until the applied retention periods

---

<sup>12</sup> Event-based retention periods require records to be retained indefinitely until a specified condition is met (e.g., a contract expires or an employee terminates), after which the record is retained for a fixed final retention period.

have expired and any *Indefinite Retention Rule* holds have been released or until the records have been transferred to another compliant storage system, (b) authorizing user privileges, and (c) maintaining appropriate technology and other information and services needed to retain the records.

## 2.3 Record Storage Verification

### 2.3.1 Compliance Requirement

The electronic recordkeeping system must automatically verify the completeness and accuracy of the processes for storing and retaining records electronically, to ensure that records read from the system are precisely the same as those that were captured.

**SEC 17a-4(f)(2)(ii) and 18a-6(e)(2)(ii):**

Verify automatically the completeness and accuracy of the processes for storing and retaining records electronically

This requirement includes both quality verification of the recording processes for storing records and post-recording verification processes for retaining complete and accurate records.

### 2.3.2 Compliance Assessment

Cohasset affirms that the functionality of Object Storage meets this SEC requirement for complete and accurate recording of records and post-recording verification processes, when the considerations identified in Section 2.3.4 are satisfied.

### 2.3.3 Object Storage Capabilities

The recording and post-recording verification processes of Object Storage are described below.

#### 2.3.3.1 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 record. If the source system transmits an MD5 hash with the record, Object Storage compares the supplied hash to its calculated hash and either (a) writes the record 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 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 records 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 repair.
  - If storage quotas are established for an account and Object Storage determines that insufficient space exists to record the record, the write process will be blocked.

### 2.3.3.2 Post-Recording Verification Process

- ▶ During retrieval of a record, 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 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 records 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.

### 2.3.4 Additional Considerations

The source system is responsible for transmitting the complete contents of the required records, and when storing a record, Cohasset recommends that the source system send a checksum to confirm a successful transmission and write of the record.

## 2.4 Capacity to Download and Transfer Records and Location Information

### 2.4.1 Compliance Requirement

This requirement calls for an adequate capacity to readily download records and information needed to locate the record in both a:

- ▶ Human readable format that can be naturally read by an individual, and
- ▶ Reasonably usable electronic format that is compatible with commonly used systems for accessing and reading electronic records.

The downloaded records and information needed to locate the records (e.g., unique identifier, index, or properties) must be transferred to the regulator, in an acceptable format.

Further, this requirement to download and transfer the complete time-stamped audit-trail applies only when this alternative is utilized; see Section 2.1, *Record and Audit-Trail*.

#### SEC 17a-4(f)(2)(iv) and 18a-6(e)(2)(iv):

Have the capacity to readily download and transfer copies of a record and its audit-trail (if applicable) in both a human readable format and in a reasonably usable electronic format and to readily download and transfer the information needed to locate the electronic record, as required by the staffs of the Commission, [and other pertinent regulators] having jurisdiction over the [regulated entity]



## 2.4.2 Compliance Assessment

It is Cohasset's opinion that the functionality of Object Storage meets this SEC requirement to maintain the capacity to readily download and transfer the records and the information used to locate the records, when the considerations described in Section 2.4.4 are satisfied.

## 2.4.3 Object Storage Capabilities

The following capabilities relate to the capacity to search, download and transfer records and the information needed to locate the records.

- ▶ Object Storage deployed in the OCI public cloud, assures that hardware and software capacity allow for ready access to the records and 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.
- ▶ Object Storage assigns a unique identifier, called an eTag, to each record and stores it as immutable metadata. Other critical attributes for the record, such as the record name, name prefixes, Bucket name, and last modified timestamp are also retained immutably. These attributes may be used as filters during the search process.
- ▶ 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 records it contains is displayed in alphabetical order by record name, along with any user-specified metadata, as key value pairs.
  - Prefixes and/or time-stamps, if utilized as part of the record naming convention, can be leveraged to filter the list of records displayed.
  - To view the contents of a record, 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 records within a Bucket, or filter the list of records within a Bucket based on prefixes and/or timestamps, if utilized as part of the record naming convention, (c) download the list of records and associated metadata attributes, (d) download selected records for viewing and/or further filtering by client-side tools, and (e) produce the records and metadata attributes.
  - Bucket-level metadata includes Bucket name, creation date, and all applied retention rule(s).
  - Record metadata includes record name, eTag, and last-modified timestamp. *Note: Calculated retention expiration dates for records are not provided by Object Storage as part of record 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 records.*

## 2.4.4 Additional Considerations

In addition, for this requirement, the regulated entity is responsible for (a) maintaining its account in good standing, (b) authorizing user privileges, (c) maintaining appropriate technology and resource capacity, encryption keys that have been used in addition to the Oracle encryption keys, and other information and services needed to

use Object Storage to readily access, download, and transfer the records and the information needed to locate the records, and (d) providing requested information to the regulator, in the requested format.

## 2.5 Record Redundancy

### 2.5.1 Compliance Requirement

The intent of this requirement is to retain a persistent alternate source to reestablish an accessible, complete and accurate record, should the original electronic recordkeeping system be temporarily or permanently inaccessible.

The 2022 final Rule amendments promulgate two redundancy options, paragraphs (A) or (B).

- ▶ The intent of paragraph (A) is:

*[B]ackup electronic recordkeeping system must serve as a redundant set of records if the original electronic recordkeeping system is temporarily or permanently inaccessible because, for example, it is impacted by a natural disaster or a power outage.*<sup>13</sup> [emphasis added]

- ▶ The intent of paragraph (B) is:

*[R]edundancy capabilities that are designed to ensure access to Broker-Dealer Regulatory Records or the SBS Entity Regulatory Records must have a level of redundancy that is at least equal to the level that is achieved through using a backup recordkeeping system.*<sup>14</sup> [emphasis added]

Note: The alternate source, must meet “*the other requirements of this paragraph [(f)(2) or (e)(2)]*”, thereby disallowing non-persistent copies that are overwritten on a periodic basis, resulting in a much shorter retention period than the original.

### 2.5.2 Compliance Assessment

Cohasset asserts that the functionality of Object Storage meets both paragraphs (A) and (B) of this SEC requirement by retaining a persistent duplicate copy of the records or alternate source to reestablish the records, when the considerations described in Section 2.5.4 are satisfied.

### 2.5.3 Object Storage Capabilities

The two options for meeting the record redundancy requirement are described in the following subsections. The method of duplicating is dependent upon the capabilities of the OCI region hosting the data as well as the size of each record.

#### SEC 17a-4(f)(2)(v) and 18a-6(e)(2)(v):

(A) Include a backup electronic recordkeeping system that meets the other requirements of this paragraph [(f) or (e)] and that retains the records required to be maintained and preserved pursuant to [§ 240.17a-3 or § 240.18a-5] and in accordance with this section in a manner that will serve as a redundant set of records if the original electronic recordkeeping system is temporarily or permanently inaccessible; or

(B) Have other redundancy capabilities that are designed to ensure access to the records required to be maintained and preserved pursuant to [§ 240.17a-3 or § 240.18a-5] and this section

<sup>13</sup> 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66421.

<sup>14</sup> 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66421.

### 2.5.3.1 Redundant Set of Records

For compliance with paragraph (A), to maintain a redundant set of records, Object Storage synchronously records three copies of each record across multiple fault domains (i.e., separate storage racks and/or storage servers and where available, across multiple data centers).

- ▶ The record is recoverable by automatically restoring the record from a duplicate located in a separate fault domain.
- ▶ The duplicate copies are retained for the full retention period of the record and any applied legal holds.
- ▶ When a Bucket's *Locked Retention Rule* is modified on primary storage (i.e., retention duration is extended), the modified retention controls *do not* propagate to the replicas. Therefore, modifications made to a primary Bucket's *Locked Retention Rule* must also be made to any replicated Buckets.

### 2.5.3.2 Other Redundancy Capabilities

For compliance with paragraph (B), Object Storage uses erasure coding to store data blocks of records redundantly. In the event of a disk failure, the original record can be regenerated.

- ▶ The record is recoverable by regenerating a duplicate of the original from erasure encoded data.
- ▶ The erasure coded data is retained for the full retention period of the record and any applied legal holds.

### 2.5.4 Additional Considerations

In addition, for this requirement, the regulated entity is responsible for: (a) maintaining its account in good standing and (b) maintaining the technology, storage capacity, encryption keys, and other information and services needed to use Object Storage and permit access to the redundant records.

Further, for Dedicated Region Cloud@Customer deployments, proper hardware sizing must be performed to ensure appropriate capacity for erasure coding and/or duplicate copies.

## 2.6 Facilities to Produce Records for Examination

### 2.6.1 Compliance Requirement

The intent of this requirement is for the regulated entity to be ready at all times (with facilities and technology) to immediately and easily provide records stored on an electronic recordkeeping system to the regulator for examination. The records may be produced as a human-readable view, print or other reproduction method that allows the regulator immediate and easy access to the requested records.

The regulator may need to use the facilities to access the records, in rare instances, such as financial failure of the regulated entity or insufficient availability of staff to respond to regulator requests to produce records.

#### SEC 17a-4(f)(3)(i) and 18a-6(e)(3)(i):

At all times have available, for examination by the staffs of the Commission, [and other pertinent regulators], facilities for immediately producing the records preserved by means of the electronic recordkeeping system and for producing copies of those records

## 2.6.2 Compliance Assessment

Cohasset affirms that Object Storage supports the regulated entity's compliance with this SEC requirement to have sufficient facilities and technology available to immediately produce human-readable renderings of the records.

## 2.6.3 Object Storage Capabilities

The regulated entity is responsible for providing adequate facilities and technology to produce records for examination, and compliance is supported by Object Storage.

- ▶ 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 records and information needed to locate the records.
- ▶ Once downloaded, local client-side capabilities may be used to render a human-readable projection or print of the records.

## 2.6.4 Additional Considerations

In addition, for this requirement, the regulated entity is responsible for (a) maintaining its account in good standing, (b) authorizing user privileges, (c) maintaining its encryption keys that have been used in addition to the Oracle encryption keys, and (d) maintaining appropriate technology, facilities and services needed to use Object Storage to readily access, download and transfer the records, and (e) providing requested records to the regulator, in the requested format.

## 2.7 Provide Records to Regulators

### 2.7.1 Compliance Requirement

This requires the regulated entity, using an electronic recordkeeping system, to immediately provide the regulator with requested records.

The records may be produced as a human-readable view, print or other reproduction method that allows the regulator immediate and easy access to the requested records.

#### SEC 17a-4(f)(3)(ii) and 18a-6(e)(3)(ii):

Be ready at all times to provide, and immediately provide, any record stored by means of the electronic recordkeeping system that the staffs of the Commission, [and other pertinent regulators] having jurisdiction over the [regulated entity] may request

### 2.7.2 Compliance Assessment

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

### 2.7.3 Object Storage Capabilities

The regulated entity is responsible for producing records for regulators, and compliance is supported by Object Storage; see Section 2.4, *Capacity to Download and Transfer Records and Location Information*, and Section 2.6 *Facilities to Produce Records for Examination*.

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

### 2.7.4 Additional Considerations

The regulated entity is responsible for providing the records to the regulator.

## 2.8 Audit System

### 2.8.1 Compliance Requirement

For electronic recordkeeping systems that comply with the non-rewriteable, non-erasable format requirement, as stipulated in Section 2.2, *Non-Rewriteable, Non-Erasable Record Format*, the Rules require the regulated entity to maintain an audit system for accountability (e.g., when and what action was taken) for both (a) inputting each record and (b) tracking changes made to every original and duplicate record. Additionally, the regulated entity must ensure the audit system results are available for examination for the required retention time period stipulated for the record.

The audit results may be retained in any combination of audit systems utilized by the regulated entity.

### 2.8.2 Compliance Assessment

Cohasset asserts that Object Storage, in conjunction with both the OCI Audit and Logging services, when enabled, supports the regulated entity's efforts to meet this SEC requirement for an audit system.

### 2.8.3 Object Storage Capabilities

The regulated entity is responsible for an audit system, and compliance is supported by Object Storage, in conjunction with both the OCI Audit and Logging services.

#### SEC 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii):

For a [regulated entity] operating pursuant to paragraph [(f)(2)(i)(B) or (e)(2)(i)(B)] of this section, the [regulated entity] 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 or § 240.18a-5] and this section to the electronic recordkeeping system and inputting of any changes made to every original and duplicate record maintained and preserved thereby.

(A) At all times, a [regulated entity] must be able to have the results of such audit system available for examination by the staffs of the Commission [and other pertinent regulators].

(B) The audit results must be preserved for the time required for the audited records

- ▶ For each record stored, Object Storage retains the following audit information.
  - Object Storage assigns a unique identifier, called an eTag, to each record.
  - The last-modified timestamp (storage date and time) is captured and stored with each record.These attributes are *immutably* stored for the lifespan of the record and are produced together with the record.
- ▶ The record is immutable, meaning changes are disallowed; therefore, tracking of the inputting of changes made is not relevant to Object Storage.
- ▶ In addition to the immutable record metadata, Object Storage offers two types of audit logging features to capture lifecycle events:
  - Bucket-level logs are captured in the OCI Audit service.
  - Record-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, including the Namespace, Compartment and Bucket where the record is stored.
  - Deleting eligible records and associated metadata, including failed attempts to delete ineligible records.
  - 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.
  - 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*).
- ▶ The OCI Audit service and Logging service retain logs in an audit index for a limited period of time and make them available via the *OCI Explore Log Groups* user interface.
  - Bucket-level audit logs can be retained for a maximum of 365 days.
  - Record-level audit logs can be retained for a maximum of 180 days.
- ▶ 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.
- ▶ Additionally, *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 and 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 records, 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., records) must be downloaded to a client-side system to view content or produce in a format and on a medium acceptable under the Rule.

## 2.8.4 Additional Considerations

The regulated entity is responsible for maintaining an audit system for inputting records. In addition to relying on the immutable metadata, the regulated entity may utilize Object Storage features alone or OCI Audit service and Logging in conjunction with another system.

## 2.9 Information to Access and Locate Records

### 2.9.1 Compliance Requirement

The intent of this requirement is for the regulated entity to maintain, keep current, and provide promptly upon request by the regulator *"all information necessary to access and locate records preserved by means of the electronic recordkeeping system."*<sup>15</sup>

#### SEC 17a-4(f)(3)(iv) and 18a-6(e)(3)(iv):

Organize, maintain, keep current, and provide promptly upon request by the staffs of the Commission, [and other pertinent regulators] having jurisdiction over the [regulated entity] all information necessary to access and locate records preserved by means of the electronic recordkeeping system

This requirement for information to access and locate the records (e.g., unique identifier, index, or properties) is designed to incorporate whatever means a particular electronic recordkeeping system uses to organize the records and locate a specific record.

### 2.9.2 Compliance Assessment

Cohasset affirms that Object Storage supports the regulated entity in meeting this SEC requirement to organize, maintain, keep current, and provide promptly the information needed to locate the records.

### 2.9.3 Object Storage Capabilities

The regulated entity is responsible for, and Object Storage supports, compliance with this requirement for information needed to locate the records.

- ▶ When records are recorded, Object Storage stores the following metadata attributes for each record:
  - **Immutable system metadata:** Critical attributes for the record, such as the record 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, 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.

<sup>15</sup> 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66424.

- ▶ Within each Bucket, records are stored in a flat storage hierarchy, however, a simulated directory structure (i.e., using a prefix string for record names, including the forward slash "/" ) may be used to help organize and search for sets of records.
- ▶ 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 records it contains is displayed in alphabetical order by record object name, along with any user-specified metadata as key value pairs.
  - Prefixes and/or timestamps, if utilized as part of the record naming convention, can be leveraged to filter the list of records displayed.
  - To view the contents of a record, 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 records within a Bucket, or filter the list of records within a Bucket based on prefixes and/or timestamps, if utilized as part of the record naming convention, (c) download the list of records and associated metadata attributes, (d) download selected records for viewing and/or further filtering by client-side tools, and (e) produce the records and metadata attributes in a format and on a medium acceptable under the Rule.
- ▶ Record metadata attributes are retained for the lifespan of the associated record.
- ▶ Bucket-level metadata attributes are retained for the lifespan of the associated Bucket.

#### 2.9.4 Additional Considerations

In addition, for this requirement, the regulated entity is responsible for:

- ▶ Assigning appropriate Bucket and record names to aid in locating records.
- ▶ Appropriately managing information that is retained separately from Object Storage and is needed to access and locate the records.

Additionally, the regulated entity is responsible for (a) maintaining its account in good standing, (b) authorizing user privileges, and (c) providing requested information to the regulator, in the requested format.

## 2.10 Designated Executive Officer or Designated Third Party Requirement

### 2.10.1 Compliance Requirement

It is the responsibility of the regulated entity to designate either an executive officer of the firm (Designated Executive Officer) or an unaffiliated third-party (Designated Third Party) to make the required undertaking.

Once the relationship is established, this requirement is the joint responsibility of the regulated entity and the designated party.

#### SEC 17a-4(f)(3)(v) and 18a-6(e)(3)(v):

(A) Have at all times filed with the [pertinent regulator] the following undertakings with respect to such records signed by either a designated executive officer or designated third party (hereinafter, the "undersigned"):

\*\*\*\*\*



In the event the regulated entity fails to download requested records and complete time-stamped audit-trails (if applicable), the designated party is required to promptly furnish the following to the regulator:

- Information deemed necessary by the regulator, and
- Downloaded copies of requested records and complete time-stamped audit-trails (if applicable), in a human readable format and a usable electronic format.

### **2.10.2 Compliance Assessment**

The regulated entity is responsible for (a) designating either an executive officer of the firm or a third-party, (b) obtaining the required undertakings, and (c) submitting the undertaking to its designated examining authority.

### **2.10.3 Object Storage Capabilities**

Complying with this requirement is the responsibility of the regulated entity.

### **2.10.4 Additional Considerations**

The regulated entity is responsible for complying with this requirement.

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

This section contains a summary assessment of the functionality of Object Storage, as described in Section 1.3, *Object Storage Overview and Assessment Scope*, in comparison to CFTC electronic regulatory record requirements. Specifically, this section associates the features described in Section 2, *Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e)*, with the principles-based requirements of CFTC Rule 1.31(c)-(d).

Cohasset's assessment, enumerated in Section 2, pertains to the electronic recordkeeping system requirements of SEC Rules 17a-4(f)(2) and 18a-6(e)(2) and the associated SEC interpretations, as well as the audit system requirement of SEC Rules 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii).

In the October 12, 2022, adopting release, the SEC recognizes the CFTC principles-based requirements and asserts a shared objective of ensuring the authenticity and reliability of regulatory records. Moreover, the SEC contends that its two compliance alternatives, i.e., (1) record and audit-trail and (2) non-rewriteable, non-erasable record format, a.k.a. WORM, are more likely to achieve this objective because each alternative requires the specific and testable outcome of accessing and producing modified or deleted records, in their original form, for the required retention period.

*The proposed amendments to Rules 17a-4 and 18a-6 and the [CFTC] principles-based approach recommended by the commenters share an objective: ensuring the authenticity and reliability of regulatory records. However, the audit-trail requirement is more likely to achieve this objective because, like the existing WORM requirement, it sets forth a specific and testable outcome that the electronic recordkeeping system must achieve: the ability to access and produce modified or deleted records in their original form.<sup>16</sup> [emphasis added]*

Cohasset's assessment, in Section 2, pertains to Object Storage, with *Locked Retention Rules*, which is a highly restrictive configuration that assures the storage solution applies integrated 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 functionality of Object Storage *Locked Retention Rules* with 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, using the *Unlocked Retention Rule*, meets these *principles-based* CFTC requirements, when the regulated entity applies appropriate procedural controls to oversee operations to remove or shorten retention periods. The first column enumerates the CFTC regulation. The second 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).

<sup>16</sup> 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.

CFTC 1.31(c)-(d) Regulation [emphasis added]	Compliance Assessment Relative to CFTC 1.31(c)-(d)
<p><i>(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:</i></p> <p><i>(1) Generally. Each records entity shall retain regulatory records in a form and manner that ensures the <u>authenticity and reliability</u> of such regulatory records in accordance with the Act and Commission regulations in this chapter.</i></p> <p><i>(2) Electronic regulatory records. Each records entity maintaining electronic regulatory records shall establish appropriate systems and controls that ensure the <u>authenticity and reliability</u> of electronic regulatory records, including, without limitation:</i></p> <p><i>(i) Systems that maintain the security, signature, and data as necessary to ensure the <u>authenticity</u> of the information contained in electronic regulatory records and to monitor compliance with the Act and Commission regulations in this chapter;</i></p>	<p>It is Cohasset's opinion that the CFTC requirements in (c)(1) and (c)(2)(i), for records<sup>17</sup> with time-based retention periods, are met by the functionality of Object Storage, when using the <i>Retention Rule</i> feature.</p> <p>The retention controls associated with <i>Locked Retention Rules</i> and features that support authenticity and reliability of electronic records are described in the following sections:</p> <ul style="list-style-type: none"> <li>● Section 2.2, <i>Non-Rewriteable, Non-Erasable Record Format</i></li> <li>● Section 2.3, <i>Record Storage Verification</i></li> <li>● Section 2.4, <i>Capacity to Download and Transfer Records and Location Information</i></li> <li>● Section 2.8, <i>Audit System</i></li> </ul> <p>Additionally, for <u>records stored electronically</u>, the CFTC definition of <u>regulatory records</u> in 17 CFR § 1.31(a) includes information to access, search and display records, as well as data on records creation, formatting and modification:</p> <p><u>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:</u></p> <p><u>(i) Any data necessary to access, search, or display any such books and records; and</u></p> <p><u>(ii) All data produced and stored electronically describing how and when such books and records were created, formatted, or modified.</u> [emphasis added]</p> <p>Object Storage retains immutable metadata attributes (e.g., unique identifier, called an eTag, and the last-modified/storage timestamp) as an integral component of the records, and, therefore, these attributes are subject to the same retention protections as the associated record. These immutable attributes support both (a) records access, search and display and (b) audit system and accountability for inputting the records. See Sections 2.4, 2.8 and 2.9 for Object Storage capabilities related to retaining information needed to search and locate the records. The most recent values of mutable metadata are retained for the same time period as the associated record.</p> <p>Further, Object Storage in conjunction with the OCI Audit and Logging services tracks audit events and provides storage options for retaining this additional audit system information for the same time period as the record. For additional information, see Section 2.8, <i>Audit System</i>.</p>

<sup>17</sup> The regulated entity is responsible for retaining and managing any additional required information, such as information to augment search and data on how and when the records were created, formatted, or modified, in a compliant manner.

**COMPLIANCE ASSESSMENT REPORT**

Oracle Object Storage: SEC 17a-4(f), SEC 18a-6(e), FINRA 4511(c), CFTC 1.31(c)-(d) and the MiFID II Delegated Regulation (72)(1)

CFTC 1.31(c)-(d) Regulation [emphasis added]	Compliance Assessment Relative to CFTC 1.31(c)-(d)
<p><i>(ii) Systems that ensure the records entity is able to produce electronic 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</i></p>	<p>It is Cohasset's opinion that Object Storage capabilities described in Section 2.5, <i>Record Redundancy</i>, including methods for a persistent duplicate copy or alternate source to reestablish the records and associated system metadata, meet the CFTC requirements (c)(2)(ii) to <u>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</u>.</p> <p>Additionally, Sections 2.5, <i>Record Redundancy</i>, and 2.9, <i>Information to Access and Locate Records</i>, explain that all Object Storage tiers (or storage classes) are designed for 99.99999999% (11 nines) of durability, using erasure coding to store data pieces redundantly across multiple disks located in different power and network failure domains.</p>
<p><i>(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.</i></p>	<p>The regulated entity is required to create and retain an <i>up-to-date inventory</i>, as required for compliance with 17 CFR § 1.31(c)(iii).</p>
<p><i>(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:</i></p> <p><i>(1) Inspection. All regulatory records shall be open to inspection by any representative of the Commission or the United States Department of Justice.</i></p> <p><i>(2) Production of <b>paper</b> regulatory records. ***</i></p> <p><i>(3) Production of <b>electronic</b> regulatory records.</i></p> <p><i>(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.</i></p> <p><i>(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.</i></p> <p><i>(4) Production of <b>original</b> regulatory records. ***</i></p>	<p>It is Cohasset's opinion that Object Storage has features that support the regulated entity's efforts to comply with requests for inspection and production of records, as described in.</p> <ul style="list-style-type: none"> <li>● Section 2.2, <i>Non-Rewriteable, Non-Erasable Record Format</i></li> <li>● Section 2.4, <i>Capacity to Download and Transfer Records and Location Information</i></li> <li>● Section 2.6, <i>Facilities to Produce Records for Examination</i>,</li> <li>● Section 2.7, <i>Provide Records to Regulators</i></li> <li>● Section 2.8, <i>Audit System</i></li> <li>● Section 2.9, <i>Information to Access and Locate Records</i></li> </ul>

## 4 • Summary Assessment of Compliance with MiFID II Delegated Regulation(72)(1)

The objective of this section is to document Cohasset's assessment of the functionality of Object Storage, as described in Section 1.3, *Object Storage Overview and Assessment Scope*, in comparison to the following requirements of the *Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing MiFID II (the MiFID II Delegated Regulation)*. Specifically, Article 72(1) defines medium and retention of records requirements:

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. [emphasis added]*

Paragraph (e), above, recognizes the technology evolution and defines requirements or conditions for regulated entities that retain records electronically. The approach is consistent with the SEC, which also sets forth standards that the electronic storage media must satisfy to be acceptable.

Additionally, the Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments (MiFID II) defines durable medium as follows:

(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]*

While the above pertains to enabling the client to store and access its information, regulated entities often apply the MiFID II durable medium requirements to internally retained information, assuring it is immutable, retained for the appropriate time period and stored in a manner that assures unchanged reproduction. For this reason, Cohasset included this citation in its analysis for this section of the report.

In the following table, Cohasset correlates specific MiFID II requirements for electronic records with the functionality of Object Storage using the *Locked Retention Rule*. In addition, Cohasset contends that Object Storage, using the *Unlocked Retention Rule*, meets these MiFID II requirements, when the regulated entity applies appropriate procedural controls to oversee operations to remove or shorten retention periods. The first column enumerates specific electronic records requirements for (a) *durable medium* in MiFID II and (b) the *medium* and

retention of records in the *Delegated Regulation*, which supplements MiFID II. The second column provides Cohasset's analysis and opinion regarding the functionality of Object Storage, relative to these requirements.

Regulatory excerpts of MiFID II media requirements [emphasis added]	Compliance assessment and analysis of Object Storage relative to these MiFID II media requirements
<p><b>Directive 2014/65/EU (MiFID II) Article 4(1)(62)</b>  <i>(62) 'durable medium' means any instrument which:</i>  <i>(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. *****</i></p> <p><b>Commission Delegated Regulation (EU) 2017/565, (the MiFID II Delegated Regulation), Article 72(1)</b>  <i>(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: *****</i></p>	<p>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.</p> <p>It is Cohasset's opinion that the <i>Retention Rule</i> feature of Object Storage applies time- based retention periods to records and associated system and custom metadata. The retention controls associated with <i>Locked Retention Rules</i> as described in Section 2.2, <i>Non-Rewriteable, Non-Erasable Record Format</i>:</p> <ul style="list-style-type: none"> <li>● Prohibit modification and overwrites for the protection period applied to the record.</li> <li>● Prohibit deletion, through any mechanism, until the assigned retention period expires and any legal holds (<i>Indefinite Retention Rules</i>) are removed.</li> </ul> <p>Further, Object Storage assures the accurate recording (storage) of the record content and associated metadata, as explained in Section 2.3, <i>Record Storage Verification</i>. The quality and accuracy of the recording process is verified: (a) during the initial recording of the record, (b) using post-recording verification during read-back, and (c) by conducting periodic consistency and integrity checking.</p>
<p><b>Directive 2014/65/EU (MiFID II) Article 4(1)(62)</b>  <i>(62) 'durable medium' means any instrument which: *****</i>  <i>(b) allows the unchanged reproduction of the information stored;</i></p> <p><b>Commission Delegated Regulation (EU) 2017/565, (the MiFID II Delegated Regulation), Article 72(1)</b>  <i>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: *****</i>  <i>(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;</i>  <i>(c) it is not possible for the records otherwise to be manipulated or altered; *****</i></p>	<p>It is Cohasset's opinion that the features of Object Storage, with <i>Locked Retention Rules</i>, achieve the non-rewriteable, non-erasable storage requirements necessary to assure that record content is unchangeable. See Section 2.2, <i>Non-Rewriteable, Non-Erasable Record Format</i>, for additional information.</p> <p>If the regulated entity corrects or amends a record in the source system, it must store each rendition as a new record. The features for non-rewriteable, non-erasable record format assure that the original record is not modified.</p> <p>Further, Object Storage calculates and retains block-level checksums during the recording process and subsequently uses it for post-recording quality and integrity checks and for automated record repair, as described in Section 2.3, <i>Record Storage Verification</i>.</p>

Regulatory excerpts of MiFID II media requirements [emphasis added]	Compliance assessment and analysis of Object Storage relative to these MiFID II media requirements
<p><b>Directive 2014/65/EU (MiFID II) Article 4(1)(62)</b>  <i>(62) ‘durable medium’ means any instrument which:</i>  <i>(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</i>  <i>(b) allows the unchanged reproduction of the information stored;</i></p> <p><b>Commission Delegated Regulation (EU) 2017/565, (the MiFID II Delegated Regulation), Article 72(1)</b>  <i>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:</i>                      *****  <i>(a) the competent authority is able to access them readily and to reconstitute each key stage of the processing of each transaction;</i>                      *****  <i>(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 *****</i></p>	<p>Cohasset asserts that Object Storage provides the following methods of retrieving records:</p> <ol style="list-style-type: none"> <li>1. Direct searches via the Object Storage console</li> <li>2. APIs</li> <li>3. CLI commands</li> </ol> <p>The selected records may be downloaded and local capabilities may be used to view, filter, print or produce in a format and on an acceptable medium. See Section 2.4, <i>Capacity to Download and Transfer Records and Location Information</i>, for additional information.</p> <p>Further, Object Storage ensures that records are readily available by ensuring persistent duplicate copies exist. Records are written to Object Storage utilizing either (a) erasure coding or (b) synchronously recording three copies of each record across multiple fault domains (i.e., separate storage racks and/or storage servers). The method of duplication is dependent upon the capabilities of the OCI region hosting the data as well as the size of each record. See Section 2.5, <i>Record Redundancy</i>, for additional information.</p>
<p><b>Directive 2014/65/EU (MiFID II) Article 4(1)(62)</b>                      N/A</p> <p><b>Commission Delegated Regulation (EU) 2017/565, (the MiFID II Delegated Regulation), Article 72(1)</b>  <i>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:</i>                      *****  <i>(e) the firm’s arrangements comply with the record keeping requirements irrespective of the technology used. *****</i></p>	<p>Cohasset asserts that Object Storage provides the following methods of retrieving records:</p> <ol style="list-style-type: none"> <li>1. Direct searches via the Object Storage console</li> <li>2. APIs</li> <li>3. CLI commands</li> </ol> <p>The selected records 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, <i>Capacity to Download and Transfer Records and Location Information</i>, for additional information. As may be required, the regulated entity may transfer records to other media or migrate records to new file formats, in advance of technological obsolescence.</p>

## 5 • Conclusions

Cohasset assessed the functionality of Object Storage<sup>18</sup> in comparison to the electronic recordkeeping system requirements set forth in SEC Rules 17a-4(f)(2) and 18a-6(e)(2) and described features that support the regulated entity as it meets the requirements of SEC Rules 17a-4(f)(3) and 18a-6(e)(3).

Cohasset determined that Object Storage, when properly configured, has the following functionality, which meets the regulatory requirements:

- ▶ Retains the records in a non-rewriteable, non-erasable format, by applying integrated control codes that prevent modifying, overwriting or deleting a record for the applied retention period.
  - *Time-bound Retention Rules* are applied to an Object Storage Bucket and *locked*, resulting in the protection of all records retained within the Bucket.
  - *Indefinite Retention Rules* are applied to an Object Storage Bucket when litigation or a subpoena requires records to be placed on hold, resulting in the indefinite protection of all records retained within the Bucket.
- ▶ Verifies the accuracy of the process for storing and retaining the records, using checksums and Object Storage validation processes.
- ▶ Retains immutable metadata, such as the unique identifier and last-modified timestamp, for the full retention period of the record.
- ▶ Retains the full text of all *Locked Retention Rules* applied to a Bucket for the lifespan of the Bucket.
- ▶ Provides capacity and tools to (a) list all Buckets or filter the list based on Bucket attributes, (b) list all records within a Bucket, or filter the list of records within a Bucket based on prefixes and/or time-stamps, if utilized as part of the record naming convention, (c) download the list of records and associated metadata attributes, (d) download selected records for viewing and/or further filtering by client-side tools, and (e) produce the records and metadata attributes in a format and on a medium acceptable under the Rule.
- ▶ Recovers an accurate replica of the records and metadata attributes from a persistent duplicate copy or regenerates a replica from erasure coded segments, should an error occur in the source record or an availability problem be encountered.

Additionally, Object Storage supports the regulated entity's compliance with the requirements defined in SEC Rules 17a-4(f)(3) and 18a-6(e)(3), by (a) retaining an audit system for non-rewriteable, non-erasable records by storing immutable metadata related to inputting each record and downloading this metadata with the associated

---

<sup>18</sup> See Section 1.3, *Object Storage Overview and Assessment Scope*, for an overview of the solution and the scope of deployments included in the assessment.



## COMPLIANCE ASSESSMENT REPORT

Oracle Object Storage: SEC 17a-4(f), SEC 18a-6(e), FINRA 4511(c), CFTC 1.31(c)-(d) and the MiFID II Delegated Regulation (72)(1)

---

record, (b) furnishing facilities to produce records for examination, (c) providing (transferring) records to the regulator for examination, and (d) maintaining information to access and locate the record.

Accordingly, Cohasset concludes that Object Storage, when properly configured and the additional considerations are satisfied, meets the electronic recordkeeping system requirements of SEC Rules 17a-4(f)(2) and 18a-6(e)(2) and FINRA Rule 4511(c), as well as supports the regulated entity in its compliance with SEC Rules 17a-4(f)(3) and 18a-6(e)(3). In addition, the assessed capabilities meet the principles-based electronic records requirements of CFTC Rule 1.31(c)-(d) and the medium and *retention of records* requirements of the *MiFID II Delegated Regulation(72)(1)*.

## Appendix A • Overview of Relevant Electronic Records 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 electronic records retained on compliant electronic recordkeeping systems.*

### A.1 Overview of SEC Rules 17a-4(f) and 18a-6(e) Electronic Recordkeeping System Requirements

In 17 CFR §§ 240.17a-3 and 240.17a-4 for securities broker-dealer industry and 17 CFR §§ 240.18a-5 and 240.18a-6 for nonbank SBS entities, the SEC stipulates recordkeeping requirements, including retention periods.

Effective January 3, 2023, the U.S. Securities and Exchange Commission (SEC) promulgated amendments<sup>19</sup> to 17 CFR § 240.17a-4 (Rule 17a-4) and 17 CFR § 240.18a-6 (Rule 18a-6), which define more technology-neutral requirements for electronic recordkeeping systems.

*The objective is to prescribe rules that remain workable as record maintenance and preservation technologies evolve over time but also to set forth requirements designed to ensure that broker-dealers and SBS Entities maintain and preserve records in a manner that promotes their integrity, authenticity, and accessibility.*<sup>20</sup> [emphasis added]

These 2022 amendments (a) provide a record and complete time-stamped audit-trail alternative and (b) allow regulated entities to continue using the electronic recordkeeping systems they currently employ to meet the non-rewriteable, non-erasable (i.e., WORM or write-once, read-many) requirement.

*Under the final amendments, broker-dealers and nonbank SBS Entities have the flexibility to preserve all of their electronic Broker-Dealer Regulatory Records or SBS Entity Regulatory Records either by: (1) using an electronic recordkeeping system that meets either the audit-trail requirement or the WORM requirement; or (2) preserving some electronic records using an electronic recordkeeping system that meets the audit-trail requirement and preserving other electronic records using an electronic recordkeeping system that meets the WORM requirement.*<sup>21</sup> [emphasis added]

The following sections separately address (a) the record and audit-trail and (b) the non-rewriteable, non-erasable record format alternatives for compliant electronic recordkeeping systems.

#### A.1.1 Record and Audit-Trail Alternative

The objective of this requirement is to allow regulated entities to keep required records and complete time-stamped record audit-trails in business-purpose recordkeeping systems.

---

<sup>19</sup> The compliance dates are May 3, 2023, for 17 CFR § 240.17a-4, and November 3, 2023, for 17 CFR § 240.18a-6.

<sup>20</sup> 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66428.

<sup>21</sup> 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66419.

*[T]o preserve Broker-Dealer Regulatory Records and SBS Regulatory Records, respectively, on the same electronic recordkeeping system they use for business purposes, but also to require that the system have the capacity to recreate an original record if it is modified or deleted. This requirement was designed to provide the same level of protection as the WORM requirement, which prevents records from being altered, over-written, or erased.<sup>22</sup> [emphasis added]*

The complete time-stamped audit-trail must both (a) establish appropriate systems and controls that ensure the authenticity and reliability of required records and (b) achieve the testable outcome of accessing and reproducing the original record, if modified or deleted during the required retention period, without prescribing how the system meets this requirement.

*[L]ike the existing WORM requirement, [the audit-trail requirement] sets forth a specific and testable outcome that the electronic recordkeeping system must achieve: the ability to access and produce modified or deleted records in their original form.<sup>23</sup> [emphasis added]*

Further, the audit-trail applies only to required records: *"the audit-trail requirement applies to the final records required pursuant to the rules, rather than to drafts or iterations of records that would not otherwise be required to be maintained and preserved under Rules 17a-3 and 17a-4 or Rules 18a-5 and 18a-6."<sup>24</sup> [emphasis added]*

### **A.1.2 Non-Rewriteable, Non-Erasable Record Format Alternative**

With regard to the option of retaining records in a non-rewriteable, non-erasable format, the adopting release clarifies that the previously released interpretations to both SEC Rules 17a-4(f) and 18a-6(e) still apply.

*The Commission confirms that a broker-dealer or nonbank SBS Entity can rely on the 2003 and 2019 interpretations with respect to meeting the WORM requirement of Rule 17a-4(f) or 18a-6(e), as amended.*

\*\*\*\*\*

*In 2001, the Commission issued guidance that Rule 17a-4(f) was consistent with the ESIGN Act. The final amendments to Rule 17a-4(f) do not alter the rule in a way that would change this guidance. Moreover, because Rule 18a-6(e) is closely modelled on Rule 17a-4(f), it also is consistent with the ESIGN Act<sup>25</sup> [emphasis added]*

In addition to the Rules, the following interpretations are extant and apply to both SEC Rules 17a-4(f) and 18a-6(e).

- *Commission Guidance to Broker-Dealers on the Use of Electronic Storage Media Under the Electronic Signatures in Global and National Commerce Act of 2000 With Respect to Rule 17a-4(f), Exchange Act Release No. 44238 (May 1, 2001), 66 FR 22916 (May 7, 2001) (2001 Interpretative Release).*
- *Electronic Storage of Broker-Dealer Records, Exchange Act Release No. 47806 (May 7, 2003), 68 FR 25281, (May 12, 2003) (2003 Interpretative Release).*
- *Recordkeeping and Reporting Requirements for Security-Based Swap Dealers, Major Security Based Swap Participants, and Broker-Dealers, Exchange Act Release No. 87005 (Sept. 19, 2019), 84 FR 68568 (Dec. 16, 2019) (2019 SBS/MSBSP Recordkeeping Adopting Release).*

---

<sup>22</sup> 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.

<sup>23</sup> 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.

<sup>24</sup> 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66418.

<sup>25</sup> 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66419.

The 2003 Interpretive Release allows rewriteable and erasable media to meet the non-rewriteable, non-erasable requirement, if the system delivers the prescribed functionality, using appropriate integrated control codes.

*A broker-dealer would not violate the requirement in paragraph [(f)(2)(i)(B) (refreshed citation number)] 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.<sup>26</sup> [emphasis added]*

Further, the 2019 interpretation clarifies that solutions using only software control codes also meet the requirements of the Rules:

*The Commission is clarifying that a software solution that prevents the overwriting, erasing, or otherwise altering of a record during its required retention period would meet the requirements of the rule.<sup>27</sup> [emphasis added]*

The term *integrated* means that the method used to achieve non-rewriteable, non-erasable preservation must be an integral part of the system. The term *control codes* indicates the acceptability of using attribute codes (metadata), which are integral to the software controls or the hardware controls, or both, which protect the preserved record from overwriting, modification or erasure.

The 2003 Interpretive Release is explicit that merely mitigating (rather than preventing) the risk of overwrite or erasure, such as relying solely on passwords or other extrinsic security controls, will not satisfy the requirements.

Further, the 2003 Interpretive Release requires the capability to retain a record beyond the SEC-established retention period, when required by a subpoena, legal hold or similar circumstances.

*[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.<sup>28</sup> [emphasis added]*

See Section 2, *Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e)*, for each SEC electronic recordkeeping system requirement and a description of the functionality of Object Storage related to each requirement.

## **A.2 Overview of FINRA Rule 4511(c) *Electronic Recordkeeping System Requirements***

Financial Industry Regulatory Authority (FINRA) rules regulate member brokerage firms and exchange markets. Additionally, FINRA adopted amendments clarifying the application of FINRA rules to security-based swaps (SBS).<sup>29</sup>

FINRA Rule 4511(c) explicitly defers to the requirements of SEC Rule 17a-4, for 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.*

---

<sup>26</sup> 2003 Interpretive Release, 68 FR 25282.

<sup>27</sup> Recordkeeping and Reporting Requirements for Security-Based Swap Dealers, Major Security-Based Swap Participants, and Broker-Dealers, Exchange Act Release No. 87005 (Sept. 19, 2019), 84 FR 68568 (Dec. 16, 2019) (2019 SBSD/MSBSP Recordkeeping Adopting Release).

<sup>28</sup> 2003 Interpretive Release, 68 FR 25283.

<sup>29</sup> FINRA, Regulatory Notice 22-03 (January 20, 2022), FINRA Adopts Amendments to Clarify the Application of FINRA Rules to Security-Based Swaps.

### A.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 modernize and make technology-neutral the form and manner in which to keep regulatory records. This resulted in less-prescriptive, principles-based requirements.

*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.<sup>30</sup> [emphasis added]*

The following definitions in 17 CFR § 1.31(a) confirm that recordkeeping obligations apply to all *records entities* and 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.

*Definitions. For purposes of this section:*

*Electronic regulatory records means all regulatory records other than regulatory records exclusively created and maintained by a records entity on paper.*

*Records entity means any person required by the Act or Commission regulations in this chapter to keep regulatory records.*

*Regulatory records means all books and records required to be kept by the Act or Commission regulations in this chapter, including any record of any correction or other amendment to such books and records, provided that, with respect to such books and records stored electronically, regulatory records shall also include:*

*(i) Any data necessary to access, search, or display any such books and records; and*

*(ii) All data produced and stored electronically describing how and when such books and records were created, formatted, or modified. [emphasis added]*

The retention time periods for required records includes both time-based and event-based retention periods. Specifically, 17 CFR § 1.31(b) 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.*

*(4) A records entity shall keep regulatory records exclusively created and maintained on paper readily accessible for no less than two years. A records entity shall keep electronic regulatory records readily accessible for the duration of the required record keeping period. [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)*.

---

<sup>30</sup> Recordkeeping, 82 FR 24482 (May 30, 2017) (2017 CFTC Adopting Release).

## A.4 Overview of the *Medium and Retention of Records* Requirements of MiFID II

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]

While the above pertains to enabling the client to store and access its information, regulated entities often apply the MiFID II durable medium requirements to internally retained information, assuring it is immutable, retained for the appropriate time period and stored in a manner that assures the unchanged reproduction.

Further, with implementation of the revised MiFID II, investment firms must arrange for records to be kept for 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.*  
[emphasis added]

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

The *MiFID II Delegated Regulation* in Section 8, *Record-keeping*, Article 72, *Retention of records*, paragraph 1, specifies:

## COMPLIANCE ASSESSMENT REPORT

Oracle Object Storage: SEC 17a-4(f), SEC 18a-6(e), FINRA 4511(c), CFTC 1.31(c)-(d) and the MiFID II Delegated Regulation (72)(1)

---

*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. [emphasis added]*

See Section 4, *Summary Assessment of Compliance with the MiFID II Delegated Regulation(72)(1)*, for a summary assessment of the capabilities of Object Storage in relation to requirements for (a) *durable medium* in MiFID II and (b) *medium and retention of records* in the *MiFID II Delegated Regulation*.

## Appendix B • Cloud Provider Undertaking

### B.1 Compliance Requirement

Separate from the electronic recordkeeping system requirements described in Section 2, *Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e)*, the SEC requires submission of an undertaking when records are stored on systems owned or operated by a party other than the regulated entity.

The purpose of the undertaking is to ensure the records are accessible and can be examined by the regulator.

SEC Rules 17a-4(i)(1)(ii) and 18a-6(f)(1)(ii) explain an 'Alternative Undertaking,' which applies to cloud service providers if the regulated entity has 'independent access' to records, which allows it to (a) regularly access the records without relying on the cloud service provider to take an intervening step to make the records available, (b) allow regulators to examine the records, during business hours, and (c) promptly furnish the regulator with true, correct, complete and current hard copy of the records.

This undertaking requires the cloud service provider (a) facilitate the process, (b) not block access, and (c) not impede or prevent the regulated entity or the regulator itself from accessing, downloading, or transferring the records for examination.

### B.2 Oracle Undertaking Process

- ▶ The undertaking requires actions be taken by both parties:
  1. The regulated entity affirms, in writing, it:
    - ◆ Is subject to SEC Rules 17a-3, 17a-4, 18a-5 or 18a-6 governing the maintenance and preservation of certain records,

#### SEC 17a-4(i)(1)(ii) and 18a-6(f)(1)(ii):

(A) If the records required to be maintained and preserved pursuant to the provisions of [§ 240.17a-3 or § 240.18a-5] and this section are maintained and preserved by means of an electronic recordkeeping system as defined in paragraph [(f) or (e)] of this section utilizing servers or other storage devices that are owned or operated by an outside entity (including an affiliate) and the [regulated entity] has independent access to the records as defined in paragraph [(i)(1)(ii)(B) or (f)(1)(ii)(B)] of this section, the outside entity may file with the Commission the following undertaking signed by a duly authorized person in lieu of the undertaking required under paragraph [(i)(1)(i) or (f)(1)(i)] of this section:

The undersigned hereby acknowledges that the records of [regulated entity] are the property of [regulated entity] and [regulated entity] has represented: one, that it is subject to rules of the Securities and Exchange Commission governing the maintenance and preservation of certain records, two, that it has independent access to the records maintained by [name of outside entity], and, three, that it consents to [name of outside entity or third party] fulfilling the obligations set forth in this undertaking. The undersigned undertakes that [name of outside entity or third party] will facilitate within its ability, and not impede or prevent, the examination, access, download, or transfer of the records by a representative or designee of the Securities and Exchange Commission as permitted under the law. \*\*\*\*\*

(B) A [regulated entity] utilizing servers or other storage devices that are owned or operated by an [outside entity or third party] has independent access to records with respect to such [outside entity or third party] if it can regularly access the records without the need of any intervention of the [outside entity or third party] and through such access:

- ( 1) Permit examination of the records at any time or from time to time during business hours by representatives or designees of the Commission; and
- ( 2) Promptly furnish to the Commission or its designee a true, correct, complete and current hard copy of any or all or any part of such records [emphasis added]



- ◆ Has independent access to the records maintained on Object Storage, and
- ◆ Consents to Oracle fulfilling the obligations set forth in this undertaking.

2. Oracle:

- ◆ Acknowledges that the records are the property of the regulated entity,
  - ◆ For the duration of its agreement with the regulated entity, agrees to facilitate within its ability, and not impede or prevent, the examination, access, download, or transfer of the records by a regulatory or trustee, as permitted under the law, and
  - ◆ Prepares the undertaking, utilizing the explicit language in the Rule, then submits, via email, the undertaking to the SEC.
- ▶ IMPORTANT NOTES: The regulated entity acknowledges that it is responsible for implementing and configuring the cloud services to ensure its records are maintained and preserved as required by applicable laws and regulations, including SEC Rules 17a-3, 17a-4, 18a-5, and 18a-6. Further, while Oracle provides this undertaking to the SEC on behalf of the regulated entity, the regulated entity is not relieved from its responsibility to prepare and maintain required records.

### B.3 Additional Considerations

The regulated entity is responsible for (a) initiating the undertaking, (b) maintaining its account in good standing, (c) implementing and configuring the cloud services to ensure its records are maintained and preserved as required by applicable laws and regulations, (d) maintaining technology, encryption keys and privileges to access Object Storage, and (e) assuring that the regulator has (when needed) access privileges, encryption keys, and other information and services to permit records to be accessed, downloaded, and transferred.

---

## About Cohasset Associates, Inc.

Cohasset Associates, Inc. ([www.cohasset.com](http://www.cohasset.com)) is a professional consulting firm, specializing in records management and information governance. Drawing on more than fifty 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, designing and supporting implementations that promote interdisciplinary information governance, achieve business objectives, optimize information value, improve compliance, and mitigate information-related risk.

Cohasset is 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.

### For domestic and international clients, Cohasset:

- *Formulates information governance implementation strategies*
- *Develops policies and standards for records management and information governance*
- *Creates clear and streamlined retention schedules*
- *Prepares training and communications for executives, the RIM network and all employees*
- *Leverages content analytics to improve lifecycle controls for large volumes of eligible information, enabling clients to classify information, separate high-value information and delete what has expired*
- *Designs and supports the implementation of information lifecycle practices that mitigate the cost and risk associated with over-retention*
- *Defines strategy and design for information governance in collaboration tools, such as M365*
- *Defines technical and functional requirements and assists with the deployment of enterprise content management and collaboration tools*

---

©2023 Cohasset Associates, Inc.

This Compliance Assessment Report and the information contained herein are copyrighted and the sole property of Cohasset Associates, Inc. Selective references to the information and text of this Compliance Assessment Report are permitted, 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 original is retained.