Cohasset Associates

IBM Cloud® Object Storage (COS)

COMPLIANCE ASSESSMENT

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

Abstract

IBM Cloud® Object Storage (COS) is a platform for storing and accessing unstructured data (objects). The *Immutable Object Storage* and *Object Lock* features (collectively referred to as IBM® Object Protection features) are designed to meet securities industry requirements for preserving records in non-rewriteable, non-erasable format for the applied retention period and legal holds.

In this report, Cohasset Associates, Inc. (Cohasset) assesses the functionality of IBM COS (see Section 1.3, *IBM COS 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 IBM COS, when properly configured and used with one of the IBM Object Protection features, has functionality that 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)(iii) and 18a-6(e)(3)(iii). Additionally, the assessed functionality of IBM COS meets the principles-based requirements of CFTC Rule 1.31(c)-(d) and the medium and retention of records requirements of the MiFID II Delegated Regulation, Article 72(1).

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.

August 2023 (v2)

12800 Whitewater Drive, Suite 100
Minnetonka, MN 55343-9347 | USA

+1.312.527.1550 | www.cohasset.com

Table of Contents

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 IBM COS 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[1], 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****[2] [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).[3]

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]

---

1 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.

2 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).

3 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*[4], 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*[5] *(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 IBM COS for preserving required electronic records, IBM® 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.

IBM engaged Cohasset to:

- Assess the functionality of IBM COS, in comparison to the electronic recordkeeping system requirements of SEC Rules 17a-4(f)(2) and 18a-6(e)(2) and describe audit system features that support the regulated entity in its compliance with SEC Rules 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii); 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 IBM COS; see Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d);*

---

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

5 *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 firms 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 IBM COS; 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 IBM COS and its functionality or other IBM products or services. The information utilized by Cohasset to conduct this assessment consisted of: (a) oral discussions, (b) system documentation, (c) user and system administrator guides, and (d) related materials provided by IBM 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 IBM COS Overview and Assessment Scope

1.3.1 IBM COS Overview

IBM Cloud Object Storage (COS) stores objects[6] in Vaults and Containers (hereinafter Buckets), which are logical containers in IBM COS. IBM COS logical storage architecture, for both the IBM Public Cloud, and IBM COS On-Premises deployments, are depicted in Figure 1:

- The **Customer Account** manages billing and other account-level activities. A single Customer Account may have many Service Instances, such as storage, compute, and other services.
- A **Service Instance** is a logical construct to manage permissions. Initiating the IBM COS Service Instance provides object storage.
- **IBM Cloud Object Storage (COS)** provides object storage services,

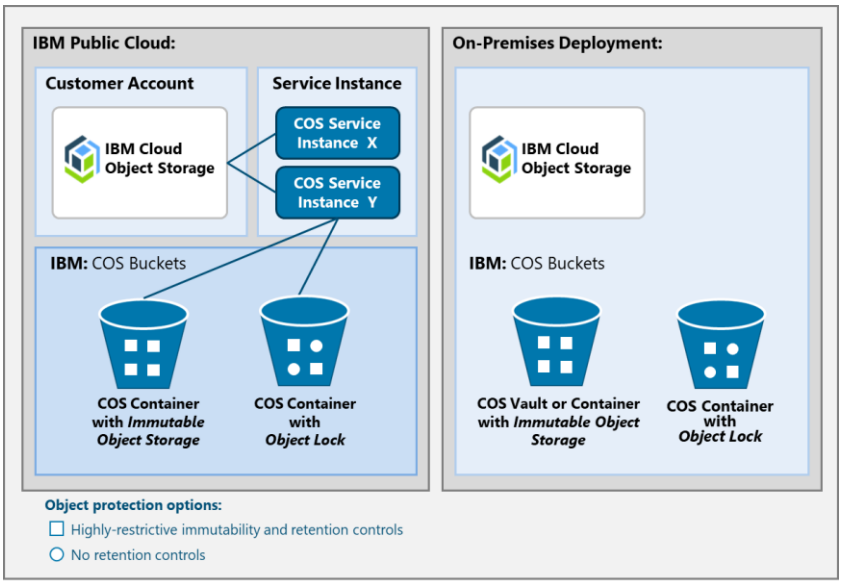

Figure 1: IBM COS logical storage architecture

6 The SEC uses the phrase books and records to describe information that must be retained for regulatory compliance. In this report, Cohasset typically uses the term record or record version (versus object, file or data) to recognize that the content may be required for regulatory compliance.

which may contain many Buckets, to retain individual objects (hereinafter *records*). The type of Bucket restricts type of retention controls that can be applied to the stored records. Specifically, the IBM COS *Immutable Object Storage* feature requires versioning to be disabled and stores records in Vaults and Containers, whereas the IBM COS *Object Lock* feature requires versioning to be enabled and stores records in Containers only. Both Vaults and Containers are referred to as Buckets in Figure 1 and in this report.

The *Immutable Object Storage* and *Object Lock* features (collectively referred to as IBM Object Protection features) were designed to meet the SEC Rule 17a-4(f) requirements to preserve electronic records as non-rewriteable, non-erasable for the required retention period and any applicable legal holds.

1.3.2 Assessment Scope

This Compliance Assessment Report pertains to IBM Cloud Object Storage, when either: (1) *Immutable Object Storage* or (2) *Object Lock* features are appropriately applied, in the following deployments:

- On-premises, Release 3.17.3
- Dedicated cloud hosted by IBM using Release 3.17.3, and
- IBM Public Cloud.

NOTE: The scope of this assessment excludes cloud services hosted by third party, other than IBM, when the third party is not affiliated with the regulated entity.

2 • Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e)

This section presents Cohasset's assessment of the functionality of IBM COS, 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 audit system requirement of SEC Rules 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii).

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 IBM COS
- ***IBM COS 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 IBM COS, as described in Section 1.3, *IBM COS Overview and Assessment Scope*, relative to the enumerated requirements of SEC Rules 17a-4(f) and 18a-6(e).

2.1 Record and Audit-Trail

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.*[7] [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.*[8] [emphasis added]

2.1.2 Compliance Assessment

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

Instead, see Section 2.2 *Non-Rewritable, Non-Erasable Record Format*, for Cohasset's assessment of IBM COS in comparison to the non-rewriteable, non-erasable record format requirement (i.e., write-once, read-many or WORM requirement), which is an alternative to this new record and audit-trail requirement.

For enhanced control, a business-purpose recordkeeping system may store records and complete time-stamped audit-trails on IBM COS, with the features and controls described in Sections 2.2 through 2.6 of this report.

2.2 Non-Rewriteable, Non-Erasable Record Format

2.2.1 Compliance Requirement

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

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*

7 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.

8 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66418.

> *a process of integrated software and hardware codes and clarified 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."*
> *****
> *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.*[9] [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 retentions periods specified in Commission rules.*[10] [emphasis added]

2.2.2 Compliance Assessment

It is Cohasset's opinion that the functionality of IBM COS, when using either: (1) *Immutable Object Storage* or (2) *Object Lock* features, meets this SEC requirement to retain records in non-rewriteable, non-erasable format for the applied time-based[11] and event-based[12] (exclusively when using *Immutable Object Storage)* 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 IBM COS Capabilities

This section describes the functionality of IBM COS 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

- The IBM COS *Immutable Object Storage* feature requires versioning to be disabled and stores records in Vaults and Containers, depending on the configurations of the deployment, whereas IBM COS *Object Lock* feature requires versioning to be enabled and stores record versions in Containers only. In this report:
  - Both Vaults and Containers are referred to as Buckets.

---

9 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66419.

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

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

12 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. IBM COS supports event-based retention only with *Immutable Object Storage* retention features; *Object Lock* features do not support event-based retention.

- The term 'record' describes the object to which retention controls may be applied. Thus, 'record' includes both (a) 'records,' when using the IBM COS *Immutable Object Storage* feature and (b) 'record versions,' when using the IBM COS *Object Lock* feature.

- Highly-restrictive retention controls, when properly configured, are applied to:
  - Records, using the IBM COS *Immutable Object Storage* feature (versioning must be disabled with *Immutable Object Storage*) or
  - Record versions, using the IBM COS *Object Lock* feature (versioning must be enabled with *Object Lock*)
- Both the *Immutable Object Storage* and *Object Lock* features are designed to apply highly restrictive retention controls to meet the requirement to preserve electronic records as non-rewriteable, non-erasable for the required retention period and any applicable legal holds. *Immutable Object Storage* and *Object Lock* cannot be enabled simultaneously on a single Bucket.
- To meet the non-rewriteable, non-erasable requirements of SEC Rule 17a-4(f), a record requiring time-based or event-based retention must:
  - be stored in a Bucket properly configured with one of the IBM Object Protection features,
  - have an appropriate retention value applied, using (a) the Bucket default, (b) an explicit retention timestamp, or (c) appropriately configured and managed event-based retention controls, and
  - apply and remove, the legal hold indicators, as appropriate.
- All attempts to modify, overwrite or delete a record (by users or source systems), prior to the expiration of the retention and legal hold controls, are rejected and added to the audit log.
  - After the retention expiration date and removal of all legal holds, the record may be modified, overwritten or deleted for *Immutable Object Storage*.
  - After the *Retain Until Date* and removal of all legal holds, the record version may be deleted for *Object Lock*.

2.2.3.2 System, Bucket and Retention Configurations

- IBM COS offers two features for applying retention controls: *Immutable Object Storage* and *Object Lock* (collectively referred to as IBM Object Protection features).
  - *Immutable Object Storage* requires versioning to be disabled and requires a one-time system configuration to set the *System Minimum, Maximum and Default retention periods*. (For the IBM Public Cloud, the System *Maximum retention period* is set by IBM.) The *Minimum and Maximum retention periods* applied to a Bucket must be within these system parameters.
  - *Object Lock* requires versioning to be enabled. *Minimum and Maximum retention periods* are not supported for Buckets with *Object Lock* enabled.
- The primary Bucket-specific configurations for the *Immutable Object Storage* and *Object Lock* features are described in the following table.

	IBM COS *Immutable Object Storage* Configurations	**IBM COS *Object Lock* Configurations**
Bucket retention control feature	● Enable *Immutable Object Storage* for the IBM COS Bucket by enabling the *Retention* protection mode. ○ The *Retention* protection mode can only be set if the Bucket is empty. ○ Once enabled for a Bucket, the *Retention* protection mode cannot be suspended or disabled.	● Enable the *Object Lock* feature (On) for the IBM COS Bucket. ○ The *Object Lock* feature can be enabled after the bucket is created, but only new versions of existing records or new records added after *Object Lock* is enabled, will be compliant with the Rule. ○ Once enabled for a Bucket, the *Object Lock* feature cannot be suspended or disabled. ● NOTE: IBM COS requires *Compliance* mode explicitly transmitted for records stored with retention controls. Transmitting a retention mode other than *Compliance* will be rejected.
Indexing	● Set indexing to *On,* for the Bucket. (This configuration is defaulted in the IBM Public Cloud.)	● Indexing is required for *Object Lock* and is enabled by default for Container Mode.
Versioning	● Set versioning to *Off* at the time of Bucket creation. ○ This configuration is only required for on-premises deployments and cloud deployments hosted by IBM. ○ Versioning cannot be enabled for Buckets configured with *Immutable Object Storage*. ○ Each record is separately managed, with separate retention and legal hold controls.	● When *Object Lock* is enabled in the bucket creation request, IBM COS automatically enables versioning for the bucket. ● When *Object Lock* is enabled after bucket is created, the user must first enable versioning. ○ Versioning cannot be disabled, once it is enabled for a Bucket with *Object Lock* enabled. ○ Each record version is separately managed, with separate retention and legal hold controls. When controls are set without specifying a version, the controls apply to the top version.
Retention controls	● Configure the Bucket with a retention policy, which defines Default, Minimum and Maximum retention periods. ○ The Bucket *Default retention period* applies when an explicit retention period is not transmitted; this assures that a retention period is applied to all records. ○ Bucket Minimum and Maximum retention periods must be within the parameters set for the system. ○ Bucket Minimum and Maximum retention periods serve as guardrails when an explicit retention period is transmitted. ● Apply either time-based or event-based retention controls to each record. ● The retention period applied to a record may be extended but cannot be shortened by any user, including the administrator. ● See Section 2.2.3.3, *Immutable Object Storage Retention Features*.	● Optionally, configure the Bucket with a *Default retention period*. Configuring a *Default retention period* is not required. ○ After a Bucket *Default retention period* is configured, the Default retention period applies to newly stored record versions, when an explicit *Retain Until Date* is not transmitted with the record version. ● Bucket Minimum and Maximum retention periods are not supported for IBM COS *Object Lock* Buckets. ● Apply only time-based retention controls to each record version. ● The *Retain Until Date* applied to a record version may be extended but cannot be shortened by any user, including the administrator. ● See Section 2.2.3.4, *Object Lock Retention Features*.
Legal holds	● Configure and then apply legal hold identifiers to individual records, when needed for litigation, government inspection or other similar circumstances. (See Section 2.2.3.6, *Legal Holds*, below, for additional information.)	● Apply the legal hold status (Y) to individual record versions, when needed for litigation, government inspection or other similar circumstances. (See Section 2.2.3.6, *Legal Holds*, below, for additional information.)

2.2.3.3 *Immutable Object Storage* Retention Features

- When using the IBM COS *Immutable Object Storage* retention feature for compliance with the non-rewriteable, non-erasable format requirement, both (a) the protection mode *(Retention)* and (b) a retention policy must be configured for a Bucket. This ensures that retention protections are applied to all records, for compliance with non-rewriteable, non-erasable format requirement.
  - The *Retention* protection mode is highly-restrictive and applies strict, integrated control codes that extend to the storage subsystem and systemically disallows administrators from shortening or removing retention protections.
    - The *retention expiration date* may be extended but never shortened.
  - Both time-based and event-based retention periods are supported.
- The Bucket retention policy is comprised of the following parameters:
  1. Bucket *Default retention period*: If the source system does not send a specific retention period with the object to be stored, then the Bucket *Default retention period* is stored as the retention value for the record.
  2. Bucket *Minimum retention period*: If the source system specifies a retention period when writing an object to be stored, the specified retention period must be greater than or equal to the *Minimum retention period* configured for the bucket. For retention extension operations, the requested extension must be greater than or equal to the current Bucket *Minimum retention period*, added to the record's creation/storage date.
     - When the retention period specified for the record is less than the *Minimum retention period*, the record is not stored, and an error message is returned.
  3. Bucket *Maximum retention period*: If the source system specifies a retention period when writing an object, the specified retention period must be less than or equal to the *Maximum Retention Period* configured for the Bucket. For retention extension operations, the requested extension must be less than or equal to the current Bucket *Maximum retention period*, added to the date/time of the extension.
     - The Bucket *Maximum retention period* must be shorter than the *System Maximum retention period*.
  4. Bucket *Enable permanent retention*: When enabled, this parameter allows a permanent retention period to be applied to records stored in the Bucket. NOTE: A permanent retention period results in the record being retained forever.
- The *Default, Minimum and Maximum retention periods* can be administratively changed at any time after initial configuration. However, these changes are not applied to previously stored records. Rather, the updated periods only apply to records stored after the policy is revised. Additionally, the current *Minimum and Maximum retention periods* apply when a record's retention period is being extended.
- **Time-based retention periods** require the record to be retained for a specified contiguous period of time from the creation or storage timestamp.

- A time-based retention period is applied to a record, using one of two methods:
  1. The Bucket *Default retention period* is applied, if the source system does not transmit an explicit retention value.
  2. If an explicit retention period or retention expiration date is transmitted with the record when it is created (stored) and if the explicit retention value is within the min/max range, it is applied to the record.

- **Event-based retention periods** or event-time-based retention periods require the record to be retained indefinitely until a specified event occurs (e.g., a contract expires or an employee terminates), after which the record must be retained for a fixed final retention period.
  - For event-based retention, the *Indefinite* retention value (-1) is applied when the record is stored. This *Indefinite* retention setting protects the record from modification, overwrite or deletion.
  - When the retention is converted to a fixed period (e.g., after the triggering event occurs), a retention period may be specified using the *Extend from Current Time* method. This causes the record's retention period to be set to the current date/time, plus the specified retention period. Alternatively, a retention period may be extended using either the *New Retention Period* or *Additional Retention Period* methods in the IBM COS API. With any retention extension, the current *Minimum and Maximum retention periods* for the Bucket are used to validate the retention period:
    - The specified retention period must be equal to or less than the current *Maximum retention period* for the Bucket.
- In addition, a record's retention period may be extended using one of four methods: (1) specifying a new retention time period, (2) adding time to the current retention time period, (3) specifying a new retention expiration date, or (4) specifying a retention period that is added to the current date/time.
  - The new retention period is compared to the current retention period and is stored only if it is greater than the current retention period.
- When a delete request is received for an individual record, the record's retention period is added to the creation/storage time to determine if the retention period has expired. See Section 2.2.3.7, *Deletion,* for additional information.

2.2.3.4 *Object Lock* Retention Features

- The IBM COS *Object Lock* feature may be enabled on the Bucket during or after Bucket creation and, once enabled, cannot be disabled by any user, including the system administrator.
  - The IBM COS *Object Lock* feature only supports and automatically applies *Compliance* mode to each record version that is protected with retention controls. At the time of this report, the IBM COS *Object Lock* feature *Governance* mode is not supported.
- When using the *Object Lock* retention feature for compliance with non-rewriteable, non-erasable format requirement:

- Bucket configurations must include both (a) the *Object Lock* feature to be enabled (On) and (b) *Versioning* must be enabled (*On*). NOTE: Assigning a *Default retention period* is optional.
- A *Retain Until Date* must be applied to each record version, either by:
  - Applying an explicit *Retain Until Date* to the record version or
  - Using the Bucket's optional *Default retention period* to calculate the *Retain Until Date*, as follows:
    - When a *Default retention period* is configured, if the record version is transmitted for storage without an explicit *Retain Until Date* and without a legal hold header, the *Default Retention Period* is added to the record version's creation/storage timestamp to calculate the *Retain Until Date*. The *Retain Until Date* is stored as metadata of the record version.
    - The *Default retention period* can be changed at any time. However, these changes are not applied to previously stored record versions. Rather, the updated *Default retention period* only applies to new record versions stored after the default is revised.
  - Accordingly, for compliance with the Rule, if the *Default retention period* is not configured, an explicit *Retain Until Date* must be transmitted with the record version.
- Only time-based retention periods are supported.

- In addition, the *Retain Until Date* applied to the record version may be extended at any time but cannot be shortened.
  - If a version ID is not specified, the updated *Retain Until Date* is applied to the current version of the record.
  - An updated explicit *Retain Until Date* is stored only if it is greater than the current *Retain Until Date*.
  - Extending the *Retain Until Date* does not generate a new record version.
- When a delete request is received for a record version, the *Retain Until Date* is compared to current time to determine if the retention control has expired. When a delete request is received for a record, without specifying a version, a delete marker is stored as the top version of the record. See Section 2.2.3.7, *Deletion,* for additional information.

2.2.3.5 Record Definition and Retention Controls

- Throughout this report, the term 'record' pertains to each unique object stored (when using *Immutable Object Storage*) or object version (when using *Object Lock*).
  - With *Immutable Object Storage,* versioning is disallowed; thus, each record is separately managed.
  - With *Object Lock,* versioning is required; thus, each record version is separately managed; in this report, when using *Object Lock*, 'record' has the same meaning as 'record version,' since each version is separately managed as a record.
- Each separately managed record, stored in an IBM COS Bucket with *IBM Object Protection* feature, is comprised of two components:

1. The complete content of the record, and
2. The record metadata attributes, including both:
   - Immutable (unchangeable) object metadata attributes, e.g., object name, creation/storage timestamp, object checksums (MD5 or SHA256 Hash), version ID (exclusively *Object Lock*) and user-specified metadata tags (which are a custom collection of name-value pairs that describe various object qualities).
   - Mutable (changeable) object metadata attributes, e.g., retention values (which may be extended but not shortened), legal hold identifiers (which may be applied and removed), object tags, access permissions and file owner.

- IBM COS offers two retention features: (1) *Immutable Object Storage* and (2) *Object Lock*.
- The following table describes the retention controls separately applied by either *Immutable Object Storage* or *Object Lock*. As a reminder, these features are mutually exclusive, meaning that a Bucket may be configured for either one, but not both, of these features. (See Section 2.2.3.2, *System, Bucket and Retention Features and Configurations,* for information on properly configuring retention controls; and for applying the controls to records, see Section 2.2.3.3, *Immutable Object Storage Retention Features,* and Section 2.2.3.4, *Object Lock Retention Features*.)

	IBM COS *Immutable Object Storage* Retention	**IBM COS *Object Lock* Retention**
Unique record identifier	● The record name must be unique for the Bucket in which it is stored. ● If the record name is not unique, the record is not stored, and an error message is reported.	● The record name and version ID must be unique for the Bucket in which it is stored. ● If the record name is not unique, a new version is stored, with a new version ID.
Applying retention controls to records	● When *Immutable Object Storage* is configured for a Bucket, highly-restrictive protections automatically apply strict, integrated control codes that extend to the storage subsystem and systemically (completely) disallow administrators from shortening or removing retention protections. ○ The retention period may be extended, though it cannot be shortened.	● When *Object Lock* is configured for a Bucket, a *Retain Until Date* must be set for a record version to apply highly-restrictive *Compliance* mode protections to the record version. The *Retain Until Date*, when set, applies strict, integrated control codes that extend to the storage subsystem and systemically (completely) disallow administrators from shortening or removing retention controls for the record version. ○ The *Retain Until Date* may be extended, though it cannot be shortened. ○ NOTE: The *Governance* mode is not supported by IBM COS *Object Lock*.
Default retention period	● A *Default retention period* must be configured for Bucket enabled with *Immutable Object Storage.* This assures that all records in the Bucket are protected with a retention value.	● If an optional *Default retention period* is configured for the Bucket enabled with *Object Lock,* records stored in the Bucket when the *Default retention period* is set can be protected with a *Retain Until Date*. ● If a *Default retention period* is not configured for the Bucket, an explicit *Retain Until Date* must be set for each record version for compliance with the non-rewriteable, non-erasable requirement. If a *Retain Until Date* is not set for the record version, it will be stored without retention controls.

	IBM COS *Immutable Object Storage* Retention	**IBM COS *Object Lock* Retention**
Modifying or overwriting records and associated metadata	● Each record and its immutable metadata are immutably stored during the applied retention period and legal holds. Thereafter, the record may be modified, overwritten or deleted. ● All attempts to **modify** or **overwrite** a record, prior to the expiration of the retention expiration date and the removal of all associated legal holds, are rejected. ○ After the retention expiration date and removal of all legal holds, the record may be **modified** or **overwritten**. If a record is **overwritten**, it is a new record with new retention attributes applied to it.	● Each record version and its immutable metadata are immutably stored during the applied retention period and legal hold status. Thereafter, the record version may be modified, overwritten or deleted. ● Versioning must be enabled; thus, attempts to **overwrite** an existing record or store a new record with the same name as a previously stored record in the same Bucket, results in storing a new version, with separately applied retention controls and legal hold controls. A new record version is stored whether or not the prior version was eligible for deletion. ● **Modifying** existing record versions, is disallowed, when retention or legal hold protections apply.
Deleting records and associated metadata	● All attempts to **delete** a record, prior to the expiration of the retention expiration date and the removal of all associated legal holds, are rejected. ● After the retention expiration date and removal of all legal holds, the record may be deleted. ○ Deleting the record also deletes its associated metadata. ● See Section 2.2.3.7, *Deletion,* for additional information.	● All attempts to **delete** a record version, prior to the expiration of the *Retain Until Date* and removal of any legal hold, are rejected. ○ After the *Retain Until Date* and removal of all legal holds, the record version may be deleted. ○ Deleting the record version also deletes its associated metadata. ● All attempts to **delete** a record without specifying the version ID results in appending a delete marker as the top version. The record can be recovered by removing the delete marker. ● See Section 2.2.3.7, *Deletion,* for additional information.
Deleting Buckets	● The Bucket cannot be deleted, unless it is empty.	● The Bucket cannot be deleted, unless it is empty.
Copying records	● A record may be **copied** between Buckets. ○ The creation timestamp of the copy reflects the date and time that the copy is stored in the destination Bucket (not the date and time the object was originally stored in the source Bucket). ○ Retention and legal hold controls can be copied over from the source record or separately applied to the new copy of the record.	● A record may be copied between Buckets. ○ Retention and legal hold controls must be separately applied to the new copy of the record.
Moving records	● A record cannot be **moved** between Buckets. Note: If moves were allowed, retention protections would be jeopardized if the new Bucket's retention features were different.	● Same as *Immutable Object Storage.*
Displaying retention controls	● To aid the system administrator, when object metadata is retrieved, the response includes: (a) retention period, (b) calculated retention expiration date, (c) retention legal hold count (number of legal hold identifiers) applied to the record, and (d) content-length.	● To aid the system administrator, when record metadata is retrieved, the response includes: (a) *Retain Until Date*, (b) legal hold attribute, and (c) content-length.

- In the IBM Public Cloud, *IBM Object Protection features* apply across all storage classes, including Standard, Vault, Cold Vault and Smart Tier. Therefore, archive policies may be used to tier records into IBM Public Cloud storage classes.

2.2.3.6 Legal Holds

When a record is subject to preservation requirements for subpoena, litigation, regulatory investigation or other special circumstances, it must be preserved immutably, i.e., any deletion, modification or overwrite must be prohibited until the hold is removed.

The following table separately describes legal hold features, specific to Buckets configured with one of the IBM Object Protection features. As a reminder, these features are mutually exclusive, meaning that a Bucket may be configured for either one, but not both, of these features; see Section 2.2.3.2, *System, Bucket and Retention Features and Configurations*.

	IBM COS *Immutable Object Storage* Legal Holds	**IBM COS *Object Lock* Legal Holds**
Applying legal holds	● When a legal hold is applied to a record in a Bucket with *Immutable Object Storage*, both a legal hold identifier (specified by the client) and the timestamp (when applied) are stored for each record. ○ Up to 100 legal holds may be applied to an individual record. ○ When protected mirror is used for the duplicate copy, if different legal holds are applied to records with the same name (same unique identifier), but in different mirrors before the mirrors are synchronized, the legal hold(s) applied to the record that was most recently updated will be retained. ● When one or more legal holds are applied to the record, immutability is enforced, and modification, overwrite and deletion of the record are prohibited, even if the retention value has expired.	● When a legal hold is applied to a record version, in a Bucket with *Object Lock*, the Boolean legal hold attribute for the specific record version is set to *Yes*. The timestamp is tracked in the IBM COS activity log; see Section 2.6, *Audit System*. ○ The legal hold status (Y) may be applied to any record version stored in a Bucket with *Object Lock*, including record versions stored without a *Retain Until Date*. ○ Note: The protected mirror feature is not supported for Buckets with *Object Lock* enabled. ● When the legal hold attribute is set to *Yes* for the specific record version, deletion of the record version is prohibited, even if the *Retain Until Date* has expired. (Note: The versioning feature, which is required to be enabled, applies immutability and protects each record version from modification or overwrite.)
Removing legal holds	● When the legal hold no longer applies to a record, the legal hold identifier (specified by the client) is removed and the legal hold timestamp is removed for each record. ● When all legal holds are removed, preservation of the record is no longer mandated by the legal hold(s); however, retention protections applied to the record continue to be enforced.	● When the legal hold no longer applies to a record version, the Boolean legal hold attribute for the specific record version is set to *No*. ● When the legal hold attribute is set to *No* for the specific record version, preservation of the record version is no longer mandated by a legal hold; however, retention controls applied to the record continue to be enforced.
Displaying legal holds	● The legal holds applied to a record are displayed with the GET (list) Object Legal Hold operation.	● The legal hold status applied to a record are displayed with the GET (list) Object Legal Hold operation.

2.2.3.7 Deletion Controls

The following table separately describes deletion eligibility, specific to Buckets configured with one of the IBM Object Protection features. As a reminder, these features are mutually exclusive, meaning that a Bucket may be configured for either one, but not both, of these features; see Section 2.2.3.2, *System, Bucket and Retention Features and Configurations*.

	IBM COS *Immutable Object Storage* Deletion Actions	**IBM COS *Object Lock* Deletion Actions**
Determining eligibility for deletion	● The record, together with its metadata, are eligible for deletion only after the three following conditions are met: ○ The records' retention period is a positive integer. NOTE: Minus one (-1) is used for an indefinite retention period and minus two (-2) is used for a permanent retention period. ○ Retention expiration date has expired (is in the past). NOTE: The retention expiration date is calculated by adding the retention period, when it is a positive integer, to the creation/storage timestamp. ○ No legal holds are currently applied to the record.	● The record version, together with its metadata, are eligible for deletion only after the two following conditions are met: ○ The *Retain Until Date* has expired (is in the past). ○ The legal hold status must be disabled (No).
Rejecting deletion, when ineligible	● Actions by permissioned users to delete an ineligible record with either an unexpired retention expiration date or an applied legal hold, are rejected.	● Actions by permissioned users to delete an ineligible record version with either an unexpired *Retain Until Date* or an applied legal hold, are rejected. ● Actions by permissioned users to delete an ineligible record (without specifying the version ID) with either an unexpired *Retain Until Date* or an applied legal hold, results in. ○ Appending a delete marker as the top version. ○ Delete markers can be removed, which results in reinstating or recovering the deleted (hidden) record.
Deleting eligible records	● Actions by permissioned users to delete an eligible record with an expired retention expiration date and not subject to a legal hold, results in record deletion.	● Actions by permissioned users to delete an eligible record version with an expired *Retain Until Date* and not subject to a legal hold, results in deletion of the record version. ● Actions by permissioned users to delete an eligible record (without specifying the version ID) with an expired *Retain Until Date* and not subject to a legal hold, results in. ○ Appending a delete marker as the top version. ○ Delete markers can be removed, which results in reinstating or recovering the deleted (hidden) record.
Deleting eligible Buckets	● A Bucket, with *Immutable Object Storage*, must be empty before it can be deleted. Accordingly, deleting a Bucket to effectuate the premature deletion of records is prohibited.	● A Bucket, with *Object Lock*, must be empty before it can be deleted. Accordingly, deleting a Bucket to effectuate the premature deletion of records is prohibited.
Deleting COS service instance	● For the IBM Public Cloud, deletion of the COS Service Instance is prohibited, if *Immutable Object Storage* features are applied to one or more Buckets.	● For the IBM Public Cloud, deletion of the COS Service Instance is prohibited, if *Object Lock* features are applied to one or more Buckets.

2.2.3.8 Security

In addition to the stringent retention and management controls described above, IBM COS provides the following security capabilities, which support the authenticity and reliability of the records.

- Role-Based Access Control security and identity and access management policies provide the means to create, delete, and maintain accounts and control user permissions.
- Encryption options for records and metadata include:
  - Transport Layer Security (TLS) is applied for network connections *within* IBM Cloud Object Storage and is supported between the upstream system and COS import operations. When used, confidentiality of data in motion is ensured.
  - Records and metadata are encrypted as the data is stored, ensuring confidentiality of data at rest.
  - Server provided encryption keys that are associated with an *Immutable Object Storage* or *Object Lock* bucket cannot be deleted. This protects immutable data from becoming inaccessible via encryption key deletion.
- Authentication is required (anonymous access is *not* supported) when an *Immutable Object Storage or Object Lock* feature is applied to the Buckets.
- The regulated entity may also choose to encrypt records prior to uploading to IBM COS. The regulated entity is responsible for maintaining its encryption keys.
- Independent third-party audits and internal IBM audits of IBM Cloud infrastructure, services and operations are undertaken on a regular basis to verify security, privacy and compliance controls.

2.2.3.9 Clock Management

- IBM COS synchronizes time with a network protocol clock (NTP) to ensure that the local clock is within a 1000 second threshold.
  - If the clock is off by less than 1000 seconds the NTP daemon begins adjusting the local clock toward the remote clock time, using drifting (slow, very small adjustments of approximately 1-2 seconds per hour) until the clocks are synchronized.
  - If the clock is off by more than 1000 seconds, the server is taken off-line and adjusted to match the remote clock and an entry is created in the audit log.
- This process ensures that timestamps are accurately recorded when the record and metadata are written, and it ensures that the clock cannot be temporarily advanced to enable the ability to prematurely delete records.

2.2.4 Additional Considerations

For this requirement, the regulated entity is responsible for enabling either: (a) *Immutable Object Storage* or (b) *Object Lock* features for IBM COS Buckets that will be used to store records required by the Rules. The additional considerations for each of these Object Protection features are enumerated in the following subsections.

2.2.4.1.1 Immutable Object Storage

In addition, when configuring and applying the *Immutable Object Storage* protection feature for compliance with this non-rewriteable, non-erasable requirement, the regulated entity is responsible for:

- Configuring Bucket retention policies with *Default, Minimum,* and *Maximum retention periods* that meet regulatory requirements, and monitoring these attributes, since changes are allowed, and the current Bucket settings are utilized to enforce retention protections when records are written and when retention periods are extended.
  - NOTE: For event-based retention, when the triggering event occurs (e.g., contract expiration), the retention period is extended from minus one (-1) to a fixed retention period. The validation of the new retention period is based on the current *Minimum retention period*. Therefore, the regulated entity must establish **procedural controls** to ensure that the *Minimum retention period* is not reset (temporarily changed) to a shortened *Minimum retention period*, as a method to allow a shortened retention period to be applied after the event has occurred.
- Applying an appropriate retention period to the records, when stored, managing event-based retention attributes, and extending the retention period, when necessary.
  - Note: In the event that the same object key is found on both sides of the mirror, but with differing content or metadata, only the object that was written most recently will be retained.
- Applying legal holds to records that require preservation for legal matters, government investigations, external audits and other similar circumstances.
  - When mirroring is used to maintain a duplicate copy of regulated records, unique legal holds must not be applied simultaneously to records with the same name (same unique identifier) to both sides of the mirror. In the event that the same object key is found on both sides of the mirror, but with differing content or metadata, only the record that was most recently updated will be retained.
- Ensuring all records required to be retained for compliance with the Rule are successfully stored in a Bucket, with *Immutable Object Storage* features, preferably within 24 hours of creation.

2.2.4.1.2 Object Lock

In addition, when configuring and applying the *Object Lock* protection feature for compliance with this non-rewriteable, non-erasable requirement, the regulated entity is responsible for:

- Enabling the *Object Lock* feature and *Versioning* on the Bucket.
- For Buckets that will store records required for compliance with the Rule, Cohasset recommends configuring an appropriate *Default retention period* to assure retention controls are applied to all records are stored in the Bucket.
- Enabling a legal hold, as needed, to preserve records for legal matters, government investigations, external audits and other similar circumstances; and, disabling the legal hold feature, when preservation is no longer required.
- Storing records requiring event-based retention periods in a compliant solution, such as a bucket configured for *Immutable Object Storage,* since the *Object Lock* feature does not support event-based retention periods.

2.2.4.1.3 IBM Object Protection Features

In addition, when either of the IBM Object Protection features are applied, the regulated entity is responsible for:

- Establishing and maintaining appropriate security controls and protocols.
- Ensuring that NTP servers are appropriately configured on IBM COS.

Additionally, the regulated entity is responsible for: (a) authorizing user privileges and (b) maintaining appropriate hardware and software, encryption keys, and other information and services needed to retain the records. Further, when using IBM Cloud Services, the regulated entity is responsible for maintaining its IBM Cloud Account in good standing and paying for appropriate services to allow records to be retained until the applied retention periods and holds have expired or until the records have been transferred to another compliant storage system.

2.3 Record Storage Verification

2.3.1 Compliance Requirement

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

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.

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 IBM COS 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 IBM COS Capabilities

The recording and the post-recording verification processes for IBM COS, are described below.

2.3.3.1 Recording Process

- As part of the record upload process, the regulated entity's source system must provide a checksum (MD5 or SHA256 Hash) of the record content. The record is only stored if the checksum calculated by IBM COS matches the checksum provided by the source system. If it does not match, the record is rejected, and an error is reported to the regulated entity (via the audit log). The record must be re-uploaded.
- When a record is successfully uploaded to IBM COS, an *Ok* response is sent to the source system.
- The checksum is stored in the record metadata. The checksum is immutable and is used in the post-recording period to verify the integrity of the record.

- Depending on the deployment storage type, IBM COS utilizes advanced electronic recording technology which applies a combination of checks and balances, such as inter-component and inter-step cyclical redundancy checks (CRCs) and write-error detection and correction, to assure that records are written in a high quality and accurate manner.

2.3.3.2 Post-Recording Verification Process

- IBM COS employs intelligent background processes that continuously scan the storage environment to identify and correct errors. In addition, the integrity of the record is validated, on each read, to ensure that an accurate record is delivered.
- If corruption is identified (i.e., the integrity check value is invalid), other non-corrupt data is used to regenerate the record.

2.3.4 Additional Considerations

- The source system is responsible for transmitting the complete contents of the required records, and Cohasset recommends:
  - The source system send a checksum enabling IBM COS to confirm the complete and accurate transmission, when inputting records.
  - HTTPS (a secure internet transfer protocol) be used, when practical, to reduce the chance of network-level errors when transmitting and inputting the records.
- For retrieval, Cohasset recommends that the source system request transmission of a checksum with the record, for validation of the transmission.

2.4 Capacity to Download and Transfer Records and Location Information

2.4.1 Compliance Requirement

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]

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*.

2.4.2 Compliance Assessment

Cohasset asserts that the functionality of IBM COS 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 IBM COS Capabilities

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

- Each record is uniquely identified:
  - For *Immutable Object Storage*, each record is uniquely identified by a combination of Bucket name and object name, which is immutably stored. If the source system attempts to store a new object with the same name as a previously stored record in the same Bucket, the write for the new object is rejected and an error message is returned. In addition, the system-generated creation/storage timestamp is immutably stored with each record.
  - For *Object Lock*, each record version is uniquely identified by a combination of Bucket name, object name and version ID. Write requests for an existing object would result in a new version of that object being created while the prior versions are maintained. In addition, the system-generated creation/storage timestamp is immutably stored with each record.
- Records and metadata attributes stored in IBM COS may be downloaded using the COS API.
- IBM COS provides GET and LIST tools to access the stored records and metadata (index) attributes.
- With the COS API, authorized users can: (a) list records and their associated metadata, (b) search the object name, and (c) download the record and associated metadata (index) attributes to a designated storage location. Record metadata (index) attributes, include:
  - Immutable object metadata, e.g., object name, version ID (exclusively *Object Lock*), creation/storage timestamp, and object size.
  - Changeable object metadata, e.g., legal hold identifiers and access control lists.

2.4.4 Additional Considerations

Additionally, the regulated entity is responsible for: (a) maintaining its account in good standing, when using IBM Cloud Services, (b) authorizing user privileges, (c) maintaining appropriate technology and resource capacity, IBM COS configurations, encryption keys, and other information and services needed to use IBM COS 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.[13] [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.[14] [emphasis added]

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

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 IBM COS meets this SEC requirement by retaining a persistent duplicate copy of the records or alternate source to reestablish the records, when (a) properly configured, as described in Section 2.5.3, and (b) the considerations described in Section 2.5.4 are satisfied.

2.5.3 IBM COS Capabilities

The two options for meeting the record redundancy requirement are described in the following subsections. The protected mirror feature, as described in Section 2.5.3.1 applies to on-premises Vault mode configurations, whereas features described in Section 2.5.3.2 apply to all configurations.

2.5.3.1 Redundant Set of Records

The protected mirror feature is available for on-premises deployments, when *Immutable Object Storage* is configured in Vault mode. The protected mirror feature is not available for the IBM Public Cloud.

13 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66421.

14 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66421.

- A protected mirror utilizes two separate Vaults, in a minimum of two data centers, each with *Immutable Object Storage* features, and creates and manages duplicate copies of the records and metadata attributes.
- A protected mirror can be configured for Synchronous or Asynchronous write modes. In both cases, records are written to both sides of the mirror simultaneously.
  - *Synchronous Mode*: A successful write message is returned to the source system, when a response is received for both write requests and one of the write requests succeeds.
  - *Asynchronous Mode*: A successful write message is returned to the source system, when a successful write response is returned from one write request.
- Neither of the two Vaults can be deleted while they are part of the protected mirror.

2.5.3.2 Other Redundancy Capabilities

The following erasure coding features apply to all configurations.

- The record and associated metadata attributes are recoverable by regenerating a duplicate of the original from erasure encoded data.
  - The erasure encoded data can be spread across multiple data centers that are geographically distant from one another.
- The erasure coded data is retained for the full retention period of the record and any applied legal holds.
- All IBM Cloud deployments utilize geo dispersal by default, and a minimum of three data centers are required for geo-dispersed cross-region storage.

2.5.4 Additional Considerations

In addition, for this requirement, the regulated entity is responsible for the following.

- When relying exclusively on erasure coding for the duplicate copy, Cohasset *recommends* the regulated entity configure the system such that the storage pools are equally distributed across three or more geographically dispersed data centers.
- For Vaults configured with *Immutable Object Storage:*
  - When using protected mirrors, where each mirror is recorded in a separate Vault, the mirrors must remain connected and must not be disassociated. If the disconnection is temporary, the vaults will synchronize when reconnected.
  - Further, with Asynchronous mode and Synchronous mode the regulated entity must ensure that each object name is unique and that two different records (with the same object name) are *not* written to each of the mirrors. Note: if records with the same name are separately written to each mirror before synchronization is completed, the record most recently updated (content or metadata) will be stored and no error will be reported.

Additionally, the regulated entity is responsible for: (a) maintaining its account in good standing, when using IBM Cloud Services and (b) maintaining the technology, storage capacity, encryption keys, and other information and services needed to use IBM COS and permit access to the redundant records.

2.6 Audit System

2.6.1 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.

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

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

2.6.2 Compliance Assessment

Cohasset asserts that IBM COS supports the regulated entity's efforts to meet this SEC audit system requirement.

2.6.3 IBM COS Capabilities

The regulated entity is responsible for an audit system and compliance is supported by IBM COS.

- For **Immutable Object Storage**, record names are a unique identifier and creation of duplicate record names is prohibited within a Bucket. If the source system attempts to store a new object with the same name as a previously stored record in the same Bucket, the write for the new object is rejected and an error message is returned.
- For **Object Lock**, immutable record attributes stored with the records are: Key Name, version ID, and creation/storage timestamp. If the source system attempts to store a new object with the same name as a previously stored record in the same Bucket, a new version of the record will be created and stored.
- Additionally, the system-generated creation/storage timestamp is immutably stored with each record.
- In addition to the immutable record metadata, activities on Buckets, with either *Immutable Object Storage* or *Object Lock,* are logged; activities include all bucket and object CRUD operations.
  - On-premises users with proper permissions have access to these logs directly.
  - For IBM Public Cloud, in addition to the immutable record metadata, the regulated entity may elect to enable the audit tracking feature and utilize the IBM tools available to export audit events; thereafter, the regulated entity may retain the audit events for the same time period as the associated record.

2.6.4 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 IBM Cloud Service features alone or in conjunction with another system.

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

This section contains a summary assessment of the functionality of IBM COS, as described in Section 1.3, *IBM COS 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.*[15] [emphasis added]

Cohasset's assessment, in Section 2, pertains to IBM COS, using either: (1) *Immutable Object Storage* or *(2) Object Lock* features, which are highly restrictive configurations that assure 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 IBM COS, using either: (1) *Immutable Object Storage* or *(2) Object Lock* features, with the *principles-based* CFTC requirements related to the *form and manner of retention* and the *inspection and production of regulatory records*. The first column enumerates the CFTC regulation. The second column provides Cohasset's analysis and opinion regarding the ability of IBM COS to meet the requirements for electronic regulatory records in CFTC Rule 1.31(c)-(d).

15 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)**
(c) Form and manner of retention. Unless specified elsewhere in the Act or Commission regulations in this chapter, all regulatory records must be created and retained by a records entity in accordance with the following requirements: *(1) Generally. Each records entity shall retain regulatory records in a form and manner that ensures the authenticity and reliability of such regulatory records in accordance with the Act and Commission regulations in this chapter.* *(2) Electronic regulatory records. Each records entity maintaining electronic regulatory records shall establish appropriate systems and controls that ensure the authenticity and reliability of electronic regulatory records, including, without limitation:* *(i) Systems that maintain the security, signature, and data as necessary to ensure the authenticity of the information contained in electronic regulatory records and to monitor compliance with the Act and Commission regulations in this chapter;*	It is Cohasset's opinion that IBM COS has features that apply time-based and event-based (*Immutable Object Storage*) or strictly time-based (*Object Lock*) retention periods to records[16] and associated system and custom metadata, as described in: ● Section 2.2, *Non-Rewriteable, Non-Erasable Record Format* ● Section 2.3, *Record Storage Verification* ● Section 2.4, *Capacity to Download and Transfer Records and Location Information* ● Section 2.6, *Audit System* Additionally, for *records stored electronically*, the CFTC definition of *regulatory records* in 17 CFR § 1.31(a) includes information to access, search and display records, as well as data on records creation, formatting and modification: *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] IBM COS retains immutable metadata attributes as an integral component of the records, and, therefore, these attributes are subject to the same retention controls 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. The immutable metadata attributes include the following (depending on configuration): ● Key Name/Document Name ● Version ID (exclusively *Object Lock*) ● Creation/storage timestamp ● MD5 hash value Additionally, mutable metadata attributes stored for records include retention controls and legal hold statuses. The most recent values of mutable metadata are retained for the same time period as the associated records.
(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	It is Cohasset's opinion that IBM COS capabilities described in Section 2.5, *Record Redundancy*, 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 *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*.

[16] 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.

CFTC 1.31(c)-(d) Regulation [emphasis added]	**Compliance Assessment Relative to CFTC 1.31(c)-(d)**
(iii) The creation and maintenance of an up-to-date inventory that identifies and describes each system that maintains information necessary for accessing or producing electronic regulatory records.	The regulated entity is required to create and retain an *up-to-date inventory*, as required for compliance with 17 CFR § 1.31(c)(iii).
(d) Inspection and production of regulatory records. Unless specified elsewhere in the Act or Commission regulations in this chapter, a records entity, at its own expense, must produce or make accessible for inspection all regulatory records in accordance with the following requirements: *(1) Inspection. All regulatory records shall be open to inspection by any representative of the Commission or the United States Department of Justice.* *(2) Production of **paper** regulatory records. **** *(3) Production of **electronic** regulatory records.* *(i) A request from a Commission representative for electronic regulatory records will specify a reasonable form and medium in which a records entity must produce such regulatory records.* *(ii) A records entity must produce such regulatory records in the form and medium requested promptly, upon request, unless otherwise directed by the Commission representative.* *(4) Production of **original** regulatory records. ****	It is Cohasset's opinion that IBM COS has features that support the regulated entity's efforts to comply with requests for inspection and production of records, as described in. ● Section 2.2, *Non-Rewriteable, Non-Erasable Record Format* ● Section 2.4, *Capacity to Download and Transfer Records and Location Information* ● Section 2.6, *Audit System*

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 IBM COS, as described in Section 1.3, *IBM COS 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 regulatory records with the functionality of IBM COS using either: (1) *Immutable Object Storage* or *(2) Object Lock* features. The first column enumerates specific electronic regulatory 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 IBM COS, relative to these requirements.

Regulatory excerpts of MiFID II media requirements [emphasis added]	**Compliance assessment and analysis of IBM COS relative to these MiFID II media requirements**
Directive 2014/65/EU (MiFID II) Article 4(1)(62) *(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* ***** **Commission Delegated Regulation (EU) 2017/565, (the MiFID II Delegated Regulation), Article 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:* *****	While this requirement pertains to the client of the regulated entity, the regulated entity itself would have a similar need to store the record for the required retention period. It is Cohasset's opinion that IBM COS has features that apply time-based and event-based (*Immutable Object Storage*) or strictly time-based (*Object Lock*) retention periods to records and associated system and custom metadata, as described in Section 2.2, *Non-Rewriteable, Non-Erasable Record Format*. The associated integrated control codes: ● Prohibit changes and overwrites during the lifespan of the record. ● Prohibit deletion, through any mechanism, until the assigned retention period expires and legal holds are removed. ● Prohibit the shortening of the retention value assigned to the record. Further, IBM COS assures the accurate recording (storage) of the record content and associated metadata, as explained in Section 2.3, *Record Storage Verification*. 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.
Directive 2014/65/EU (MiFID II) Article 4(1)(62) *(62) 'durable medium' means any instrument which:* ***** *(b) allows the unchanged reproduction of the information stored;* **Commission Delegated Regulation (EU) 2017/565, (the MiFID II Delegated Regulation), Article 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:* ***** *(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;* *****	It is Cohasset's opinion that the features of IBM COS to achieve non-rewriteable, non-erasable storage meet this requirement to assure that record content is unchangeable. Specifically, when retention controls are applied, IBM COS inherently requires each corrected or amended record to be stored as either a new record (when using *Immutable Object Storage*) or as a new record version (when using *Object Lock*). This assures that the original record is not modified. Separate retention and legal hold controls apply to each record and record version. See Section 2.2, *Non-Rewriteable, Non-Erasable Record Format*, for additional information. Further, IBM COS 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, *Record Storage Verification*.

Regulatory excerpts of MiFID II media requirements [emphasis added]	**Compliance assessment and analysis of IBM COS relative to these MiFID II media requirements**
Directive 2014/65/EU (MiFID II) Article 4(1)(62) *(62) 'durable medium' means any instrument which:* *(a) enables a client to store information addressed personally to that client in a way accessible for future reference and for a period of time adequate for the purposes of the information* *(b) allows the unchanged reproduction of the information stored;* **Commission Delegated Regulation (EU) 2017/565, (the MiFID II Delegated Regulation), Article 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;* ***** *(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* *****	Cohasset asserts that IBM COS provides direct searches via REST APIs for retrieving records. The selected records may be downloaded and local capabilities may be used to view or print the records. See Section 2.4, *Capacity to Download and Transfer Records and Location Information*, for additional information. Further, IBM COS ensures that records are readily available by writing the data using erasure coding which assures that a replica can be accurately regenerated from erasure coded data should an error occur in any segment of the data, or an availability problem be encountered in any one facility. See Section 2.5, *Record Redundancy*, for additional information.
Directive 2014/65/EU (MiFID II) Article 4(1)(62) *N/A* **Commission Delegated Regulation (EU) 2017/565, (the MiFID II Delegated Regulation), Article 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:* ***** *(e) the firm's arrangements comply with the record keeping requirements irrespective of the technology used.* *****	Cohasset asserts that IBM COS provides direct searches via REST APIs for retrieving records. The selected records may be downloaded and local capabilities may be used to view or print the records. See Section 2.4, *Capacity to Download and Transfer Records and Location Information*, for additional information. The regulated entity may transfer records to other media or migrate records to new file formats, in advance of technological obsolescence.

5 • Conclusions

Cohasset assessed the functionality of IBM COS[17], with both: (1) *Immutable Object Storage* and *(2) Object Lock* features, in comparison to the electronic recordkeeping system requirements set forth in SEC Rules 17a-4(f)(2) and 18a-6(e)(2) and described audit system features that support the regulated entity as it meets the requirements of SEC Rules 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii).

Cohasset determined that IBM COS, when properly configured with either: (1) *Immutable Object Storage* or *(2) Object Lock* features, has the following functionality, which meets the regulatory requirements:

- Retains records and immutable record metadata in a non-rewriteable, non-erasable format for time-based and event-based retention periods, when *Immutable Object Storage* or *Object Lock* features are applied.
- Applies legal holds to preserve records for a subpoena, legal hold or similar circumstances as immutable and prohibits deletion or overwrites until the legal hold is removed.
- Prohibits deletion of a record and its immutable metadata until the associated retention period has expired and any applied legal hold has been removed.
- Encrypts records at rest and within the IBM network and supports encryption for records transmitted for storage.
- Verifies the accuracy of the process for storing and retaining records, utilizing a checksum (MD5 or SHA256 Hash), which is received from the source system during the recording process and is stored as a metadata attribute and utilized for post-recording verification.
- Provides authorized users with the capacity and tools to readily find, access and download the records and information needed to locate the records for a browser or other local tool to render a human readable view and produce in the requested electronic format.
- Meets the requirement for redundancy through erasure coding or protected mirrors (available exclusively for Vaults configured with *Immutable Object Storage)*.
- Supports the regulated entity's obligation to retain an audit system for non-rewriteable, non-erasable records.

Accordingly, Cohasset concludes that IBM COS, when properly configured, including use of *Immutable Object Storage* or *Object Lock* features, 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 the audit system requirements in SEC Rules 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii). 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)*.

[17] See Section 1.3, *IBM COS Overview and Assessment Scope*, for an overview of the solution and the scope of deployments included in the assessment.

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[18] 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.*[19] [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.*[20] [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.

[18] The compliance dates are May 3, 2023, for 17 CFR § 240.17a-4, and November 3, 2023, for 17 CFR § 240.18a-6.

[19] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66428.

[20] 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.*[21] [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.*[22] [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."*[23] [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****[24] [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 SBSD/MSBSP Recordkeeping Adopting Release).

---

21 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.
22 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.
23 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66418.
24 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.*[25] [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.*[26] [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.*[27] [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 IBM COS 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).[28]

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.*

---

25 2003 Interpretative Release, 68 FR 25282.

26 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).

27 2003 Interpretative Release, 68 FR 25283.

28 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.*[29] [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 IBM COS in relation to each requirement, see Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*.

[29] 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:

> *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 IBM COS 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 the 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.

These undertakings are designed to address the fact that, while the broker-dealer or SBS Entity has independent access to the records, the third party owns and/or operates the servers or other storage devices on which the records are stored. Therefore, the third party can block records access. In the Alternative Undertaking, the third party will need to agree not to take such an action. Further, the third party will need to agree to facilitate within its ability records access. This does not mean that the third party must produce a hard copy of the records or take the other actions that are agreed to in the Traditional Undertaking. Rather, it means that the third party undertakes to provide to the Commission

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]

representative or designee or SIPA trustee the same type of technical support with respect to records access that it would provide to the broker-dealer or SBS Entity in the normal course.[30] [emphasis added]

B.2 IBM Undertaking Process

- Customers interested in obtaining an Alternative Undertaking for Cloud Service Providers for IBM Cloud Object Storage can open a support case using their IBM Cloud account portal.
- Through the process, the regulated entity will be asked to affirm it:
  - Is subject to SEC Rules 17a-3, 17a-4, 18a-5, or 18a-6 governing the maintenance and preservation of certain records,
  - Has independent access to the records maintained on IBM COS, and
  - Consents to IBM fulfilling the obligations set forth in this undertaking.
- IBM will prepare the undertaking, utilizing the explicit language in the Rule, and either provide the undertaking to the regulated entity or to the SEC.
  - IMPORTANT NOTE: This action by IBM does not relieve the regulated entity from its responsibility to prepare and maintain required records.

B.3 Additional Considerations

The regulated entity is responsible for (a) initiating a support case for the undertaking, (b) maintaining its account in good standing, (c) maintaining technology, encryption keys and privileges to access IBM COS, (d) 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, and (e) ensuring the undertaking is submitted to the SEC.

30 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66429.

About Cohasset Associates, Inc.

Cohasset Associates, Inc. (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.

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*

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.