One Microsoft Way
Redmond, WA 98052-6399

Microsoft Corporation Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

May 3, 2023

ABC Advisors, Inc.
1234 Main Street
Chicago, IL 60631

RE: Attestation of Electronic Storage Media, SEC Rule 17a-4(f)(2)(i)

To whom it may concern:

ABC Advisors, Inc. ("Company") has entered into a volume licensing agreement, incorporating the Online Services Terms ("Agreement"), with Microsoft Corporation or an affiliate of Microsoft Corporation ("Microsoft") for some or all of the Microsoft 365 and/or Immutable Storage for Azure Blobs services described in the attached Appendices (Appendix A: SEC 17a-4(f) & CFTC 1.31(c)-(d) Compliance Assessment, Microsoft 365, and Appendix B: SEC 17a-4(f) & CFTC 1.31(c)-(d) Compliance Assessment, Microsoft Azure Storage) (collectively, "Services"). In order to be eligible for, and rely upon, this letter (including all Appendices, "Letter"), Company must maintain an active subscription for Services, acquire and maintain all appropriate subscription licenses, and comply with the Agreement and this Letter.

Microsoft's Services offer cloud-based archiving solutions that allow companies to implement one or more policies for the retention of regulated communications content. The Appendices describe the specific Services that Company may configure to meet SEC Rule 17a-4(f)(2)(i) requirements and also how to configure those Services to satisfy these requirements. Company determines the categories of communications and files it retains through the Services, in accordance with the system configurations it has selected and implemented. As described in the Appendices, these categories may be affected by changes to the Agreement, changes to the configuration settings Company selects, and the extent of implementation by Company. Microsoft does not undertake to provide updates with respect to changes to the Agreement (including expiration or termination of the Agreement), the Company's configuration settings, or the Company's system implementation to FINRA, the U.S. Securities and Exchange Commission, the Commodity Futures Trading Commission, or other regulators or designated examining authorities.

As required by Rule 17a-4(f)(2)(i) under the Securities Exchange Act of 1934, Microsoft hereby represents that the Services, when used in accordance with the Agreement and this Letter, and when compliance features are properly configured, carefully applied and managed as described in the Appendices, enable Company to:

- preserve its records exclusively in a non-rewriteable, non-erasable format;
- verify automatically the quality and accuracy of the storage media recording process;

- serialize the original and, if applicable, duplicate units of storage media, and time-date for the required period of retention the information placed on such electronic storage media; and
- have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable under Rule 17a-4(f), as required by the U.S. Securities and Exchange Commission or the self-regulatory organizations of which Company is a member.

For clarity, Company is still responsible for notifying, in accordance with any required notice period, its applicable examining authority prior to implementing any electronic storage media (including the Services), and otherwise ensuring compliance with Rule 17a-4.

Upon termination or expiration of Company's subscription to the Services, Microsoft will retain the records Company designated to be archived in the Services, and that remain stored in the Services, in a limited function account accessible by Company for a defined retention period in accordance with the terms of the Agreement. After the initial retention period ends, Microsoft will disable the limited function account and proceed to delete Company's data in accordance with the terms of the Agreement, unless prohibited to do so by applicable law.

Should you have any questions regarding the foregoing, please contact Archiving in Microsoft Online Services at One Microsoft Way, Redmond, WA 98052, Attention: Archiving in Microsoft Online Services Attestation of Electronic Storage Media, or by e-mail at **FSIAssist@microsoft.com.**

Very truly yours,

Michael Ziock

Mike Ziock
Partner Director, Service Engineering
Microsoft Corporation

Cohasset Associates

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

Microsoft 365 (SharePoint, OneDrive, Teams, Exchange and Skype)

BENEFIT FROM COHASSET'S INDUSTRY INSIGHT AND EXPERIENCE

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

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

Abstract

Microsoft 365 is a cloud-based platform that provides user productivity applications and services. Certain Microsoft 365 applications, in conjunction with key features of the *compliance center,* apply integrated controls to meet securities industry requirements for preserving certain electronic records in a non-rewriteable, non-erasable format for the duration of applied retention periods and legal holds.

In this Report, Cohasset Associates, Inc. (Cohasset) assesses the capabilities of Microsoft 365 services relative to:

- The recording, storage and management requirements for electronic records, as specified by:
  - Securities and Exchange Commission (SEC) in 17 CFR § 240.17a-4(f), which regulates exchange members, brokers or dealers.
  - ♦ Financial Industry Regulatory Authority (FINRA) Rule 4511(c), which defers to the format and media requirements of SEC Rule 17a-4(f).
- The principles-based electronic records requirements of the Commodity Futures Trading Commission (CFTC) in 17 CFR § 1.31(c)-(d).

When compliance features are properly configured and carefully applied and managed, as described in this Assessment Report, it is Cohasset's opinion that the assessed Microsoft 365 services (see Section 1.3, *Microsoft 365 Overview and Assessment Scope),* meet the five requirements related to the recording and non-rewriteable, non-erasable storage of electronic records. Key actions for achieving compliance include (a) applying a combination of *regulatory record labels and/or retention policies* with *preservation lock,* (b) applying *eDiscovery holds* to records, as needed, and (c) storing records in Microsoft 365 services: (i) Exchange (often referred to as Outlook), including *Skype for Business* peer-to-peer instant messaging and web conferencing transcripts; Teams channel messages; and, Teams chats; (ii) SharePoint document libraries; or (iii) OneDrive for Business document libraries. Further, the assessed Microsoft 365 services support the regulated entities' efforts to achieve compliance with the remainder of the seventeen requirements of the Rule. Additionally, the assessed capabilities of Microsoft 365 meet the principles-based requirements of CFTC Rule 1.31(c)-(d).

Table of Contents

1 | Introduction

Regulators, world-wide, establish explicit requirements for regulated entities that elect to retain books and records[7] *on electronic storage media. Given the prevalence of electronic books and records, these requirements apply to most broker-dealer and commodity futures trading firms and other organizations with similarly regulated operations.*[2]

This Introduction *briefly summarizes the regulatory environment pertaining to this assessment, explains the purpose and approach for Cohasset's assessment, provides an overview of Microsoft 365 and the scope of this assessment, and presents an executive summary.*

1.1 Overview of the Regulatory Requirements

1.1.1 SEC Rule 17a-4(f) Requirements

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

> *The Commission is adopting a rule today which, instead of specifying the type of storage technology that may be used, sets forth standards that the electronic storage media must satis[v to be considered an acceptable method of storage under Rule 1 la-4.*[3] [emphasis added]

Further, the SEC issued two Interpretive Releases (No. 34-44238 on May 1, 2001, and No. 34-47806 on May 7, 2003), which pertain specifically to the electronic storage media requirements of paragraph (f).

For additional information, refer to Section 5.1, *Overview of SEC Rule 7 la-4({) Electronic Records Storage Requirements*.

1.1.2 FINRA Rule 4511(c) Requirements

Financial Industry Regulatory Authority (FINRA) Rule 4511(c) explicitly defers to the format and media requirements of SEC Rule 17a-4, for the books and records it requires.

> *All books and records required to be made pursuant to the FINRA rules shall be preserved in a format and media that complies with SEA [Securities Exchange Act] Rule 1 la-4.*

[1] Regulators use the phrase *books and records* to describe information about certain business transactions, customers, personnel and other administrative activities that must be retained under the Rules. Where feasible, Cohasset used the term *record* to recognize that the data or object is a regulated record.

[2] Throughout this report, Cohasset uses the phrase *regulated entity* to refer to organizations required to retain records according to the media requirements of the SEC, FINRA or the CFTC. Specifically, Cohasset uses *regulated entity* instead of *records entity,* which the CFTC defines as "any person required by the Act or Commission regulations in this chapter to keep regulatory records."

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

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

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

Refer to Section 3, *Summary Assessment of Compliance with CFTC Rule 7.37(c)-(d),* which correlates the CFTC principles-based requirements to the capabilities of the assessed Microsoft 365 services, as described in Section 2. Additionally, refer to Section 5.3, *Overview of CFTC Rule 7.37(c)-(d) Electronic Regulatory Records Requirements.*

1.2 Purpose and Approach

To obtain an independent and objective assessment of the compliance capabilities of the assessed Microsoft 365 services, Microsoft engaged Cohasset Associates, Inc. (Cohasset). As a highly-respected consulting firm, Cohasset has recognized expertise and more than 40 years of experience with the legal, technical and operational issues associated with the records and information management practices of companies regulated by the SEC and the CFTC. Additional information about Cohasset is provided in the last section of this report.

Microsoft engaged Cohasset to:

- Assess the capabilities of certain Microsoft 365 services, in comparison to the seventeen requirements of SEC Rule 17a-4(f) for recording, storage and management of electronic records; see Section 2, *Assessment of Compliance with SEC Rule 77a-4(f);*
- Associate the principles-based requirements of CFTC Rule 1.31(c)-(d) to the assessed capabilities of Microsoft 365 services; see Section 3, *Summary Assessment of Compliance with CFTC Rule 7.37(c)-(d);* and
- Prepare this Assessment Report, enumerating the results of its assessment.

In addition to applying the information in this Assessment Report, regulated entities must ensure that the combination of its policies, procedures and regulatory submissions, in conjunction with the capabilities of implemented electronic recordkeeping solutions, meet all applicable requirements.

This assessment represents the professional opinion of Cohasset and should not be construed as either an endorsement or a rejection by Cohasset of Microsoft 365 services or other Microsoft products or services. The information utilized by Cohasset to conduct this assessment consisted of: (a) oral discussions, (b) system documentation, (c) technical articles, and (d) other directly-related materials provided by Microsoft 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 Microsoft 365 Overview and Assessment Scope

Microsoft 365 is a cloud-based platform that provides user productivity applications and services. Within Microsoft 365, the *compliance center* portal is used to configure key compliance features such as *retention policies, regulatory record labels,* and *eDiscovery holds,* which work in conjunction with other Microsoft 365 applications to apply integrated controls to manage records.

This assessment pertains to certain electronic records that are managed by Microsoft 365 services when appropriate compliance features are properly configured and applied to the content stored in: (a) Exchange (often referred to as Outlook), including communications stored in Exchange, i.e., *Skype for Business* peer-to-peer instant messaging and web conferencing transcripts, Teams channel messages, and Teams chats; (b) SharePoint document libraries; or (c) OneDrive[4] document libraries.

To enable compliance with the SEC Rule 17a-4(f) requirement for a non-rewriteable, non-erasable record format, the compliance retention features listed in the grey rows in the following table must be applied to regulated records. Legacy policies (e.g., default policy tags, retention policy tags and personal policy tags), are excluded from this assessment.

The following table enumerates the compliance retention features that have been assessed for compliance (grey rows), the applicable Microsoft 365 locations[5] and the content that is included and excluded for each location.

Microsoft 365 location	*Included* in the assessment	*Excluded* from the assessment
Retention policies **with** ***preservation lock***[6] **or** ***Regulatory record labels*** **published in** ***label policies*** **with** ***preservation locK***		
• SharePoint sites	• SharePoint site document libraries, including communication sites, team sites and classic sites, whether or not associated with a Microsoft 365 Group. • Records shared in Teams channel messages. • Records shared in Teams sites. • Teams meeting recordings, when stored in SharePoint.	• SharePoint **lists** and attachments associated with list items. • Other SharePoint assets, such as wiki, tasks, biogs, etc.
• OneDrive accounts	• OneDrive document libraries. • Records shared in **1:1** and 1:many Teams chats. • Records shared in OneDrive, including files shared via a link in an electronic mail message. • Teams private meeting recordings when stored in OneDrive.	• OneDrive assets other than the document library.

[4] Throughout this report, Cohasset has used 'OneDrive' to describe 'OneDrive for Business,' a Microsoft 365 service.

[5] Locations are Microsoft 365 services where a *retention policy* or *regulatory record label* can be applied.

[6] The *retention policy(ies)* documented in this report must be configured through the *compliance center* and the *preservation lock* feature must be applied to these *retention policy(ies),* using PowerShell, for compliance with SEC Rule 17a-4(f).

[7] The *retention label(s)* documented in this report must be configured through the *compliance center* and the *regulatory record label* option must be selected. Further, when the *regulatory record label* is published, the *preservation lock* feature must be applied to the *label policy(ies),* using PowerShell. These configurations are required for compliance with SEC Rule 17a-4(f),

Microsoft 365 location	***Included* in the assessment**	***Excluded* from the assessment**
Regulatory record labels* published in *label policies* with *preservation lock		
• Exchange[8] **user or shared** mailboxes • NOTE: See below for use of *retention policies* for Exchange calendar entries, group mailboxes, public folders and other messages (e.g., Skype and Teams) stored in Exchange	• Sent and received electronic mail messages stored in **user or shared** mailboxes (excluding **qroup** mailboxes, which are only supported by *retention policies).*	• Group, site and resource mailboxes. • User and shared mailbox items other than sent and received electronic mail messages. (Calendar entries, tasks, notes, and contacts are examples of excluded items.) • Members of distribution lists, when more than 10,000 members or more than 25 nested levels. • Read receipts. • Reactions (e.g., likes/thumbs up) applied to mailbox items.
Retention policies* with *preservation lock		
• Exchange **user or shared** mailboxes	• Sent and received electronic mail messages and calendar entries stored in **user or shared** mailboxes.	• Group, site and resource mailboxes. (See the next row for **group** mailboxes.) • **User or shared** mailbox items other than electronic mail messages and calendar entries. (Tasks, notes, and contacts are examples of excluded items.) • Members of distribution lists, when more than 10,000 members or more than 25 nested levels. • Read receipts. • Reactions (e.g., likes/thumbs up) applied to mailbox items.
• Exchange **group** mailboxes, including mail-enabled groups, and SharePoint sites connected to group	• Received electronic mail messages and calendar entries stored in **group** mailboxes, including **group** mailboxes automatically generated during Teams setup. • SharePoint sites connected to a group. • NOTE: Only *retention policies* can be applied to **group** mailboxes; and, the *retention policy* applied to the **group** automatically applies to both the **group** mailbox and the connected SharePoint site. Additionally, *retention labels,* including *regulatory record labels,* may be published to the **group's** SharePoint site.	• Members of distribution lists, when more than 10,000 members or more than 25 nested levels. • Read receipts. • Reactions (e.g., likes/thumbs up) applied to mailbox items.

[8] Exchange is often referred to as Outlook. Exchange is the back end service; and, Outlook is used to access mailbox items stored in Exchange.

Microsoft 365 location	*Included* in the assessment	*Excluded* from the assessment
• Exchange public folders	• Exchange public folders items.	• No items are excluded.
• Skype for Business[9]	• Peer-to-peer instant messaging and web conferencing transcripts, when stored in hidden folders in the Microsoft 365 Exchange service.	• Peer-to-peer file transfers. • Audio and video recordings for peer-to-peer instant messages and conferences. • Desktop and application sharing (i.e., screen sharing) for peer-to-peer instant messages and conferences. • User status updates posted to *What's happening today*. • Other Skype for Business collaboration elements *not* stored in the Microsoft 365 Exchange service.
• Teams channel messages for a given Team within a tenant	• Teams channel messages stored in hidden folders in the Microsoft 365 Exchange service.	• Teams private channel messages. • Read receipts. • Note: For emojis, giffies (GIFs), memes and stickers, only weblinks are captured; and, these may change over time.
• Teams 1:**1** and **1**:many chats[10]	• **1**:1 and 1:many chats for authenticated users are stored in hidden folders in the Microsoft 365 Exchange service.	• Teams chats exclusively among guests.[11] • Teams chats on an external tenant. • Also see exclusions listed above for Teams channel messages.

Additionally, Reactions (e.g., likes, thumbs up) applied to Teams channel messages and Teams chats are tracked in the Microsoft 365 unified audit system, which regulated entities may export and store in a compliant location for regulatory compliance.

For clarity, this Compliance Assessment does not pertain to (a) Teams meeting content that is not stored in Exchange, SharePoint or OneDrive, (b) Yammer and Yammer messages, (c) Stream, (d) Live Events through Yammer, Teams, and/or Stream, (e) audio recordings for the European Union MiFID II compliance, (f) Planner, (g) Whiteboard, (h) SharePoint Lists, (i) Praise, Polls and other Microsoft or third-party applications, and U) other content not explicitly listed in the preceding tables.

[9] Skype for Business content that may be stored in the conversation history file in Exchange, is in addition to the compliance copy archived in the Microsoft 365 Exchange service; therefore, the conversation history file is not relevant to this assessment.

[10] Microsoft Teams channel messages and Teams chats stored in the chat service are in addition to the compliance copy archived in the Microsoft 365 Exchange service; therefore, the chat service is not relevant to this assessment.

[11] Chats exclusively among guests are stored in the Exchange mailboxes associated with the Guest accounts in your tenant. While these chats are discoverable, neither retention policies nor retention labels may be applied, at this time.

1.4 Executive Summary

This *Executive Summary* highlights key features for compliance with SEC Rule 17a-4(f). It is not a substitute for the remainder of this Assessment Report.

Microsoft 365 is a cloud-based platform that provides user productivity applications and services. Within Microsoft 365, the *compliance center* provides purpose-built solutions to manage different compliance needs, including Information Governance, Records Management and eDiscovery, among others. Through these solutions, authorized users define *retention policies, regulatory record labels,* and *eDiscovery holds* (legal holds). These features are designed for: (1) retaining records, (2) preserving records for legal holds, such as subpoena or litigation, (3) protecting records in a *non-rewriteable, non-erasable format [for the required retention period and applicable legal holds]* in compliance with SEC Rule 17a-4(f)(2)(ii)(A), and (4) optionally, automating the deletion of eligible records.

This Assessment Report focuses on these compliance features and how they are executed within Microsoft 365 services: (a) SharePoint document libraries, (b) OneDrive document libraries and (c) Exchange.

- To enable compliance with the non-rewriteable, non-erasable requirement, the compliance retention features listed in the following table must be applied to regulated records. As of the date of this report, for each location, *only* the listed compliance retention feature has been assessed for compliance. See Section 1.3, *Microsoft 365 Overview and Assessment Scope,* for details related to each location.

***Compliance center* retention features**	**Microsoft 365 location**
Retention policy, with *preservation lock*	• SharePoint site document libraries • OneDrive account document libraries • Exchange **user, shared or group** mailboxes[12] for sent and received electronic mail messages and calendar entries • Exchange public folders • Skype for Business peer-to-peer instant messaging and web conferencing transcripts, when stored in an Exchange mailbox • Teams channel messages, when stored in an Exchange mailbox • Teams chats, when stored in an Exchange mailbox
Regulatory record labels published in a *label policy* with *preservation lock*	• SharePoint site document libraries • OneDrive account document libraries • Exchange **user or shared** mailboxes for sent and received electronic mail messages only

- A *retention policy* *automatically* applies to all versions of files/items in the location, including new versions which may continue being created. When a *retention policy* is applied, users cannot delete versions from the version history. In contrast, a *regulatory record label* is applied by a user. Once applied, all existing versions are protected, but new versions cannot be created. Before a *regulatory record label* is applied, users may delete versions. See Section 2.1.4, *Additional Considerations,* in the *Non-Rewriteable, Non-Erasable Record Format* section, for information on managing versions.

- When a *retention policy* with *preservation lock,* a *regulatory record label* or an *eDiscovery hold* are properly applied to a record stored in the assessed services:

[12] The *retention policy* with *preservation lock* applied to a group will automatically apply to the group mailbox and the connected SharePoint site. For example, Teams setup automatically creates a group mailbox and a connected SharePoint site.

- The record content is immutable.
- Key properties and metadata attributes, such as creation (storage) timestamp and the universal identifier (ItemID for Exchange and GUID for SharePoint and OneDrive) are immutable. Additionally, *regulatory record labels* apply immutability controls to user-maintained metadata, such as the asset identifier used for event-based retention and the subject field for electronic mail messages.
- A *retention policy* cannot be removed from the location, after applying *preservation lock,* and a *regulatory record label* cannot be removed from the record, after applied. Further, the associated retention durations can only be extended and cannot be shortened. These controls apply to all users, including administrators, which assures the applied retention period cannot be shortened or circumvented.

These immutability protections apply until the respective retention period expires or the *eDiscovery hold* is removed.

- The retention periods set for the policies and labels must meet or exceed the retention requirements established by regulators and self-regulatory organizations, e.g., FINRA.
  - Time-based[13] retention periods are supported by both *retention policies* and *regulatory record labels.*
  - Event-based[14] retention periods are supported by *regulatory record labels,* when the asset identifier is added prior to applying the *regulatory record label.*
  - *Preservation lock* must be applied to the *retention policies* and *label policies* that publish *regulatory record labels,* to provide required compliance protections and eliminate methods of circumventing the retention period after it is applied.
- As summarized in the table, on the preceding page and detailed in Section 1.3, *Microsoft 365 Overview and Assessment Scope:*
  - Only *retention policies* can be applied to group mailboxes (*retention labels,* including *regulatory record labels* cannot be applied to group mailboxes). Further, Teams setup automatically configures both a group mailbox and a connected SharePoint site, and any *retention policy* applied to the group applies to both the group mailbox and associated SharePoint site. Therefore, if the group retains email messages needed for compliance with the SEC Rule, a *retention policy,* with *preservation lock,* must be applied to the group, which will automatically apply the *retention policy* to the associated SharePoint site. Additionally, *regulatory record labels* may also be published to the SharePoint site.
  - When *retention policies* are applied to **user or shared** mailboxes, the policy applies to both electronic mail messages and calendar entries; in contrast, *regulatory record labels* may be applied only to electronic mail messages (not calendar entries or other mailbox items).
- After a *retention policy,* with *preservation lock,* is applied to a location, record content is automatically protected for compliance. Individual users are not required to take additional steps.

[13] Time-based retention periods require the record to be retained for a fixed, contiguous period of time calculated from the date created/stored or the date last modified.

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

- In contrast, *regulatory record labels* must be either:

  1. Manually applied to individual files and electronic mail messages, as an explicit label, or
  2. Manually applied to a container for it to automatically apply to records stored in the container, when the record does not have an existing *retention label.* Examples of containers include: (a) a folder in Exchange or (b) a document library, folder or document set in SharePoint or OneDrive.

  NOTE: At the time of this assessment, features to auto-apply *regulatory record labels* are not available, though they may be offered in the future.

- Only one *retention label* can apply to a file or electronic mail message at a time:

  - When a record without a *retention label* is placed in the container, it inherits the label closest in the hierarchy.
  - When a record has an explicit,[15] implicit,[16] or persistent[17] *retention label,* it must be manually removed before the record will inherit the *regulatory record label* previously applied to the container hierarchy.

  IMPORTANT NOTES:

  - This distinction is critical, because the action of moving a file to a container with a *regulatory record label* will not assure the container's *regulatory record label* is inherited by the file. Instead, the *regulatory record label* will only apply if no explicit or persistent label currently applies to the file.
  - Further, if the label is a *regulatory record label* or a *record label* (e.g., a *retention label* with *classify as a record),* the inherited label attaches to the file as if it were explicitly applied.

- The record content and key properties, such as creation (storage) timestamp and the universal identifier (ItemID for Exchange and GUID for SharePoint and OneDrive) are immutable and cannot be modified, overwritten or deleted until (a) the applied retention periods have expired and (b) any *eDiscovery holds* are removed.

- When a *retention policy* is applied to a record:

  - If the record is **moved** from the document library or Exchange mailbox, it is **copied** to the destination location and then deleted from the source destination, where it originally resided. The deleted record is retained in the hidden archive[18] until it is eligible for deletion.
  - If the record is **deleted** (by a user or by a lifecycle process) before the applied retention period has expired, the record is retained in a hidden archive until both (a) applied *retention policies* expire (the longest *retention policy* wins) and (b) *eDiscovery holds* are removed.
  - Further, applying *preservation lock* to the *retention policy* assures that the *retention policy* cannot be removed from the location (site/account/mailbox) and the *retention policy's* retention period cannot be shortened, disallowing means of circumventing the retention requirement of the *retention policy.*

[15] Explicit labels were manually applied directly to the file/item.

[16] Implicit labels were inherited by the file from a library, folder or document set.

[17] Persistent labels were previously inherited, i.e., were previously implicitly applied. Thus, if a file/item is *moved* out of a folder where a label was inherited, the label will persist for the file/item. Then, if a new label is applied to the new folder where the file/item with the persistent label resides, the new label will overwrite the persistent label.

[18] The hidden archive for Exchange is the recoverable items folder and is the preservation hold library for SharePoint and 0neDrive.

- When a *regulatory record label* is applied, the record cannot be deleted from the SharePoint site, OneDrive account or Exchange user or shared mailbox until the retention period of the applied *retention label* expires.
  - If the record is **deleted** after the *regulatory record label's* retention period expires and continued retention is required by a *retention policy* or an *eDiscovery hold,* the record is retained until it is no longer required by all applied *retention policies* and *eDiscovery holds*.
  - A record with a *regulatory record label* can be **moved** only within the library or mailbox where it is stored.
  - Further, a *regulatory record label,* itself, cannot be deleted and the retention duration can only be extended and cannot be shortened.
- When an *eDiscovery hold* applies to an existing record, before the record is updated, a copy of the record is added to the hidden archive, where it is retained until both (a) applied *retention policies* expire (the longest *retention policy* wins) and (b) *eDiscovery holds* are removed.
- User and lifecycle processes to delete a SharePoint site or OneDrive account are blocked, until all associated files are deleted.
- Point-in-time *restores* of a SharePoint site or OneDrive account are blocked if either (a) a *regulatory record label* is published to the site/account or (b) *retention policy* with *preservation lock* is applied to the site/account.
- User and lifecycle processes to delete an Exchange user, shared or group mailbox that is storing electronic mail messages, Skype for Business or Teams communications with ongoing retention or eDiscovery hold requirements, will result in marking the mailbox as *inactive,* rather than being deleted. See subsection 2.1.3.2 *Compliance Retention Features,* specifically subsection 5, *Special Handling,* for additional information.
- Microsoft manages and applies encryption policies and the customer key (if this service is used by the regulated entity) to encrypt and decrypt records and associated properties and metadata attributes. Additionally, the regulated entity is responsible for managing and using its own encryption keys.
- Microsoft 365 services are cloud-based and are designed for high (99.9%) availability and site resilience. Each Exchange mailbox, along with its properties and metadata (index attributes), are replicated across at least two, and up to four, data centers. SharePoint and OneDrive stores records, along with its properties and metadata (index attributes), in erasure coded segments, which are replicated.
- The creation (storage) timestamp, unique identifier and version identifier serialize each record. These attributes are system-generated and cannot be edited by users or administrators.
- *Content search* capabilities, for eDiscovery managers and other authorized users, are robust and allow for extensive searches, as well as narrowing the search results through refined query terms.
  - Sites/accounts/mailboxes cannot be removed from *content search*.
  - *Content search* queries metadata attributes for files/items in SharePoint, OneDrive, and Exchange including content that is visible to the user and also hidden archives. Full-text search queries all extracted text from emails and attachments in Exchange, the first and top (current) version from SharePoint and OneDrive document libraries, and files/items in the hidden archives.
  - Recycle Bin content is not indexed for content search.

- Records identified in a search may be reviewed and downloaded, together with key properties and metadata (index attributes).
- Authorized users may search for, select, open, view and download records using either:
  - Web applications, which require only an Internet connection and a local computer, laptop, smartphone or other compatible device.
  - Installed applications on the users' computers, laptops and other compatible devices, as part of the Microsoft 365 license agreement.
- Human-readable renditions of the stored records are generated using the source application or a viewer. Downloads are in native or standard formats, such as Personal Storage Table (PST), Word and Excel files.
  - Teams channel messages are stored as conversation segments, which may be rethreaded as a download option.
  - Emojis, giffies (GIFs), memes and stickers are stored as weblinks, which may change over time.
  - Reactions (e.g., likes/thumbs up) applied to Teams channel messages and Teams chats are tracked in the Microsoft 365 unified audit system. To retain this information for regulatory compliance, regulated entities must (a) export the audit activities to a file that is stored it in a compliant solution for the required retention period and (b) assure that the source message also has appropriate retention and compliance controls applied to it.
  - Reactions (e.g., likes/thumbs up) applied to electronic mail messages are not retained in Exchange and are excluded from this assessment.
- When downloading records:
  - Microsoft 365 Exchange message content, properties and metadata attributes are downloaded, by default.
  - SharePoint and OneDrive record content, properties and metadata attributes (e.g., author title, creation/ storage timestamp, and last modified timestamp) are downloaded with the record, by default.
  - Several reports document the process, including, but not limited to, an Export Summary, Manifest and Results log for each exported item, and Trace Log with details of the export process.
- The availability period for audit activities in the Microsoft 365 unified audit system ranges between 90 days and 10 years, depending on subscription options. Additionally, Microsoft features enable the regulated entity to export audit activities; thereafter, the regulated entity may store these audit activities in a separate system to meet the requirement to retain audit activities for the same time period as the associated record.
  - Audit activities concerning creation, e.g., creation timestamp, author or sender, recipients (for communications), are automatically captured as system-maintained metadata.
  - By default, audit activities in the Microsoft 365 unified audit system is extensive. In addition to these defaults, the *ApplyRecord* activity in Exchange must be enabled for the mailbox administrator, delegate and owner, which will add these audit activities to the unified audit system.

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

The following subsections document Cohasset's assessment of the capabilities of relevant Microsoft 365 services, when compliance features are properly configured and used, relative to each requirement of SEC Rule 17a-4(f).

This section presents Cohasset's assessment of the capabilities of the assessed Microsoft 365 services, for compliance with the seventeen requirements related to recording, storage and management of electronic records, as stipulated in SEC Rule 77a-4(f}.

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

- ***Compliance Requirement-*** Excerpt of each electronic storage requirement in SEC Rule 17a-4(f) and Cohasset's interpretation of the requirement
- ***Compliance Assessment-Assessment*** of the relevant capabilities of Microsoft 365 services
- ***Capabilities of the Assessed Microsoft 365 Services*** - Description of relevant capabilities
- ***Additional Considerations*** - Additional considerations related to meeting the specific requirement

The following subsections document Cohasset's assessment of the capabilities of relevant Microsoft 365 services, as described in Section 1.3, *Microsoft 365 Overview and Assessment Scope,* relative to each requirement of SEC Rule 17a-4(f).

2.1 Non-Rewriteable, Non-Erasable Record Format

2. 1.1 Compliance Requirement [SEC 17a-4(f)(2)(ii)(A)J

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

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

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

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

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

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

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

2.1.2 Compliance Assessment

It is Cohasset's opinion that the assessed Microsoft 365 services (see Section 1.3 *Microsoft 365 Overview and Assessment Scope),* with the *retention policy* and *regulatory record label* features (with *preservation lock*), meets this SEC requirement to retain records in non-rewriteable, non-erasable format for the applied retention period and any associated legal holds, when (a) properly configured and applied, as described in Section 2.1.3, and (b) the considerations described in Section 2.1.4 are satisfied.

2.1.3 Capabilities of the Assessed Microsoft 365 Services

This subsection describes the capabilities of the assessed Microsoft 365 services that directly pertain to this SEC requirement for preserving electronic records as non-rewriteable, non-erasable, for the required retention period and any associated legal holds.

2.1.3.1 Overview

- The Microsoft 365 *compliance center* provides access to solutions to manage compliance needs, including information governance and records management. Through these solutions, authorized users define *retention policies,*[19] *regulatory record labels,*[20] and *eDiscovery holds* (legal holds). These features, together with *preservation lock,* are designed to: (1) retain records, (2) preserve records for legal holds, such as subpoena and litigation, (3) protect records in a non-rewriteable, non-erasable format [for the required retention period and applicable legal holds/ in compliance with SEC Rule 17a-4(f)(2)(ii)(A), and (4) optionally, automate deletion of eligible records.
- The controls to protect the records in a non-rewriteable, non-erasable format for the specified retention period are applied and enforced by each specific Microsoft 365 location, which ***result in different behaviors.*** As of the date of this report, only the *compliance center* features described for each location in the table in Section 1.3, *Microsoft 365 Overview and Assessment Scope,* have been assessed for compliance with SEC Rule 17a-4.
- A *retention policy* is applied to a SharePoint site, OneDrive account or Exchange mailbox and it governs stored files, sent and received electronic mail messages and calendar entries, whereas the *regulatory record label*

[19] For compliance with SEC Rule 17a-4(D, the *retention policy* must be configured through the *compliance center* and the *preservation lock* feature must be applied to it.

[2o] For compliance with SEC Rule 17a-4(f), the *retention label* must be configured through the *compliance center* and the *regulatory record label* option must be selected. Further, when the *regulatory record label* is published, the *preservation lock* feature must be applied to the *label policy*.

attaches to the file or electronic mail message and stays with the file/message. This important distinction is described in detail in Section 2.1.3.2, *Compliance Retention Features.*

- When a *retention policy* with *preservation lock,* a *regulatory record label* or an *eDiscovery hold* are properly applied to a record stored in the assessed services:

  - The record content is immutable, and
  - Key properties and metadata attributes, such as creation (storage) timestamp and the universal identifier (ItemID for Exchange and GUID for SharePoint and OneDrive) are immutable. Additionally, *regulatory record labels* apply immutability controls to user-maintained metadata, such as the asset identifier used for event-based retention and subject for electronic mail messages.
  - A *retention policy* cannot be removed from the location, after applying *preservation lock,* and a *regulatory record label* cannot be removed from the record, after applied. Further, the associated retention durations can only be extended and cannot be shortened. These controls apply to all users, including administrators, which assures the applied retention period cannot be shortened or circumvented.

  These immutability protections apply until the respective retention period expires and/or any associated *eDiscovery holds are* removed. For additional information, see Section 2.1.3.3, *Compliance Retention Features,* below.

2.1.3.2 Compliance Retention Features

The *compliance center* provides two compliance retention features: (1) *retention policies* and (2) *retention labels* (specifically *regulatory record labels) which are published for use by label policies.* Further, *preservation lock* applies additional controls to assure compliance. See Section 1.3, *Microsoft 365 Overview and Assessment Scope,* for the retention feature assessed for each Microsoft 365 location.

1. Retention Policies with Preservation Lock

- For compliance with the non-rewritable, non-erasable requirement of SEC Rule 17a-4(f), *retention policy(ies),* with *preservation lock,* must be (a) configured in the *compliance center,* (b) set with an appropriate time-based[21] retention period (retain action) and optional delete action, (c) locked with the *preservation lock* feature, and (d) applied as described in this subsection. A properly configured and applied *retention policy,* with *preservation lock,* automatically protects stored records through integrated control codes; additional user action is not required. A *retention policy,* with *preservation lock* ensures:

  - The *retention policy* cannot be deleted.
  - The retention duration set for the policy cannot be shortened; its duration can only be extended.
  - Locations cannot be removed from the policy; only new locations can be added.

  These controls apply to all users, including administrators.

[21] Time-based retention periods require the record to be retained for a fixed, contiguous period of time calculated from the date created/stored or last modified. Event-based retention periods are not supported by *retention policies*.

- A *retention policy* applies time-based[22] retention periods and immutability protections as follows:
  - Once applied to a location, record content is automatically protected for compliance. Individual users are not required to take additional steps.
  - If a record is **moved** from the document library or Exchange mailbox, it is **copied** to the destination location and then deleted from the source destination, where it originally resided. The deleted record is retained in the hidden archive until it is eligible for deletion.
  - If a record is **deleted** (by a user or by a lifecycle process) before the applied retention period has expired, the record is retained in a hidden archive[23] until both (a) applied *retention policies* expire (the longest *retention policy* wins) and (b) *eDiscovery holds* are removed.
  - A record version cannot be overwritten, modified or deleted by users or by lifecycle processes until expiration of the associated retention period. (New record versions may be created; see subsection *3. Versions,* below, for additional details.)
    - ♦ Before users' edits are stored for electronic mail messages, calendar entries, and Skype and Teams communication, the original is automatically saved in the hidden archive, where it is immutably retained for its lifespan.
    - For files/records in SharePoint and OneDrive document libraries, immutability protections are achieved by retaining *every* version of the file. Therefore, new file versions may be created and stored.
  - Key properties and metadata attributes, such as creation (storage) timestamp and the universal identifier (ItemID for Exchange and GUID for SharePoint and OneDrive) are immutable. Other file properties and metadata attributes may be updated, particularly when new versions are created.
- If multiple *retention policies* apply to a record, it is retained in either the site/account/mailbox or the hidden archive until all applicable retention and hold requirements have expired. Note: When a *regulatory record label* also applies to the record, it remains in the site/account/mailbox until the period of the *retention label* expires. (See subsection 2, *Regulatory Record Labels,* below.)
- When records are **deleted** (by a user or by another policy), but ongoing retention is required by a *retention policy* or *eDiscovery hold,* each of the existing versions of the record are separately retained in the associated hidden archive until the *longest* retention period expires and all *eDiscovery holds* are removed. (See subsection *3. Versions,* below, for more details.) Note: When a *regulatory record label* also applies to the record, it remains in the site/account/mailbox until the period of the *retention label* expires. (See subsection 2, *Regulatory Record Labels,* below.)
- User and lifecycle processes to delete a SharePoint site or OneDrive account are blocked, until all associated records are deleted. User and lifecycle processes to delete an Exchange user, shared or group mailbox results in marking the mailbox as *inactive,* rather than being deleted. (See subsection *5. Special Handling,* for additional information.)

[22] Time-based retention periods may be based on the creation or last modified timestamp, and disposition eligibility is calculated based on the current (top) version or the individual version, depending on storage location.

[23] The hidden archive for Exchange is the recoverable items folder and is the preservation hold library for SharePoint and 0neDrive.

2. Regulatory Record Labels

- For compliance with the non-rewritable, non-erasable requirement of SEC Rule 17a-4(f), *regulatory record labels* must be (a) configured in the *compliance center,* (b) set with an appropriate time-based or event-based retention period (with a retain action), (c) marked as a *regulatory record label,* (d) published in *label policies* with *preservation lock,* and (e) applied to records as described in this subsection. A properly configured and applied *regulatory record label,* protects stored records through integrated control codes, which ensure:

  - The *regulatory record label* cannot be deleted.
  - The retention duration set for the label cannot be shortened, its duration can only be extended.
  - Labels and locations cannot be removed from the *label policy* with *preservation lock;* only new labels and locations can be added.
  - A SharePoint site, OneDrive account or Exchange mailbox, cannot be deleted, until the associated records are deleted. NOTE: The *regulatory record label* may be applied only to (a) files/records in SharePoint and OneDrive document libraries (though not other types of content, e.g., lists and wikis) and (b) electronic mail messages, only, in Exchange user or shared mailboxes. See Section 1.3, *Microsoft 365 Overview and Assessment Scope,* for additional information.

  These controls apply to all users, including administrators.

- A *regulatory record label* applies either time-based[24] or event-based[25] retention periods and immutability protections as follows:

  - The *regulatory record label* cannot be removed from a record, once applied. Individual users, site collection administrators, users with records management roles, and users with other roles are *unable* to remove the label from the record.
  - Files/items with a *regulatory record label* cannot be deleted until the retention period applied by the *regulatory record label* has expired.
  - Files/items with a *regulatory record label* can only be **moved** within the SharePoint or OneDrive library or within the Exchange mailbox where it exists. The *regulatory record label* remains applied after the record is moved. NOTE: For SharePoint and OneDrive, when the file is moved, all existing file versions move as a unit.
  - New versions of a record cannot be created; and, all of the record versions are immutably retained and cannot be overwritten, changed or deleted by users or by lifecycle processes, until eligible for deletion. For SharePoint and OneDrive, the protections apply until the top (current) version is eligible for deletion, after which the file and its versions may be deleted. For Exchange, deletion eligibility is separately calculated for the current and prior versions.
  - Key properties and metadata attributes, such as creation (storage) timestamp and the universal identifier (ItemID for Exchange and GUID for SharePoint and OneDrive) are immutable. Additionally, user-

[24] Time-based retention periods may be based on the date and time of creation, last modification or application of the retention label and disposition eligibility is calculated based on the current (top) version or the individual version, depending on storage location.

[25] Event-based retention periods are triggered by entering the date and time the event occurred.

maintained metadata, such as the asset identifier used for event-based retention and the subject for electronic mail messages, are immutable.

- User and lifecycle processes to delete a SharePoint site or OneDrive account are blocked, until all associated records are deleted. User and lifecycle processes to delete an Exchange user, shared or group mailbox results in marking the mailbox as *inactive,* rather than being deleted. (See subsection *5. Special Handling,* for additional information.)

- Only one *retention label* can apply to a file or electronic mail message at a time. For compliance with the Rule, a *regulatory record label* must be applied by the user by either:

1. Manually applying the *regulatory record label* to the individual file or electronic mail message in a user or shared mailbox, as an explicit label, or

2. Manually applying the *regulatory record label* to a container. (Containers include (a) user created folder in Exchange, or (b) a document library, folder or document set in SharePoint or OneDrive.) Then, assuring that the records added to the container inherit[26] the *regulatory record label.* Therefore, if a record has an explicit,[27] implicit,[28] or persistent[29] *retention label,* it must be manually removed before the record will inherit the *regulatory record label* previously applied to the container hierarchy.

   NOTE: At the time of this assessment, features to auto-apply *regulatory record labels* are not available, though they may be added in the future.

- Since only one label can apply at a time, only files, without a *retention label,* will inherit the label closest in the hierarchy.

  - A file **uploaded** from a source outside of Microsoft 365 will not have a *retention label* and, therefore, it will inherit the label closest in the hierarchy.

  - When a file is **copied** within Microsoft 365, the application of a *retention label* to the new copy varies depending on the type of *retention label* applied to the original file.

    - If a *regulatory record label* or *record label (i.e., a retention label* with *classify as a record)* is applied to the original file, it will not be applied to the new copy, because the copy would be immutable (unchangeable). However, the label in the folder hierarchy (if any exist) would apply to the new copy.

    - If a standard *retention label* (i.e., not a *regulatory record label* nor a *record label)* is applied to the original file, it may automatically apply to the new copy.

  - When a file/item is **moved** from within Microsoft 365 and has a previously applied explicit or persistent *retention label,* the existing *retention label* needs to be manually removed before the file/item will inherit the *regulatory record label* previously applied to the container hierarchy.

[26] A *regulatory record label* that is inherited attaches to the file/item as if it were explicitly applied.

[27] Explicit labels were manually applied directly to the file/item.

[28] Implicit labels were inherited by the file from a library, folder or document set.

[29] Persistent labels were previously inherited, i.e., were previously implicitly applied. Thus, if a file/item is *moved* out of a folder where a label was inherited, the label will persist for the file/item. Then, if a new label is applied to the new folder where the file/item with the persistent label resides, the new label will overwrite the persistent label.

These scenarios and distinctions are critical, because the action of moving or copying a file/item to a container with a *regulatory record label* will not assure the *regulatory record label* will apply. Instead, the *regulatory record label* will apply only if a *retention label* is not currently applied to the file/item. To aid in monitoring the application of *retention labels,* the Microsoft 365 *content explorer* displays a current view of applied retention labels and the *activity explorer* displays a history of labeling activities.

I/VIPORTANT NOTE: When a *regulatory record label* is inherited, the label attaches to the file/item, as if it were explicitly applied, and once applied, it is cannot be removed.

- *Regulatory record labels* support time-based retention periods, which are based on record creation (storage) timestamp. Additionally, event-based retention periods (wherein the fixed retention period begins to accrue after an event, e.g., after account closure) are also supported, when the asset identifier is added as metadata prior to applying the *regulatory record label.*

3. Versions

- Versions are stored to support collaboration in SharePoint and OneDrive document libraries. Currently, Microsoft automatically configures 500 major versions for a new document library. The default version configuration can be overridden. SharePoint Library Settings allows a range of 100-50,000 major versions.
- Storing versions also supports compliance, as described in the following table.

	Retention policy* or *eDiscovery hold	***Regulatory record label***
• Maintain immutable record content	• A *retention policy* with a retain action or an eDiscovery hold automatically saves each version of the record, including versions that exceed the version configuration for the library. o For SharePoint and OneDrive, new versions are created when the record contents are modified. o For Exchange, a new version is created when the subject, body, attachments, senders and recipients or sent and received dates are modified. NOTE: A new version is not created when the organizer receives responses from attendees and the meeting tracking information is updated. • Since all versions are stored, retention of shared versions is assured.	• After a *regulatory record label* is applied to a record, no existing versions can be deleted. Additionally, a subsequent version cannot be created: o In SharePoint and OneDrive, all existing versions of the record are locked (immutably protected) by the *regulatory record label.* Therefore, to make edits, the record must be saved as a new record. o In Exchange, the electronic mail message is locked (immutably protected) by the *regulatory record label;* versions in the hidden archive are separately managed.
• Maintain immutable file properties and metadata (index attributes)	• Key properties and metadata attributes, such as creation (storage) timestamp and the universal identifier (ItemID for Exchange and GUID for SharePoint and OneDrive) are immutable.	• Key properties and metadata attributes, such as creation (storage) timestamp and the universal identifier (ItemID for Exchange and GUID for SharePoint and OneDrive) are immutable. • User-maintained metadata, such as the asset identifier used for event-based retention and the subject for electronic mail messages are immutable.

	Retention policy* or *eDiscovery hold	***Regulatory record label***
• Protect against premature deletion	• If a record is **deleted** by users or by lifecycle processes, a *retention policy* or *eDiscovery hold* automatically saves the record and its existing versions in the hidden archive. • For records in the hidden archive, each version is separately stored and managed.	• A *regulatory record label* prohibits deletion from the primary site/mailbox until the retention period associated with the label has expired. Thereafter, if a *retention policy* or *eDiscovery hold* applies to the record, see the middle column.

- Versions of files/records may also need to be retained to support shared links, i.e., cloud attachments.[30] Specifically, when a file is shared in Teams channel messages or Teams chats, only a link is shared; the file is not embedded in the communication message. In Outlook (the user software for Exchange), the user can select to embed a copy of the file or share a link. When the shared file is required for regulatory compliance, steps must be taken to assure that the version that is shared is retained as a regulatory record in compliance with Rule 17a-4(f), as described in this Assessment Report.

4. Deletion Actions

- A record retained by a *regulatory record label* cannot be deleted from the site/account/mailbox until the retention period of the applied *regulatory record label* has expired. (Only one *regulatory record label* may apply to a record.)
- A record retained by a *retention policy* may be manually deleted by the user, to remove it from the user's active view; however, this moves the file to the hidden archive, if ongoing retention is required by a *retention policy* or *eDiscovery hold*. (Multiple *retention policies* and/or *eDiscovery holds* may apply to a record.)
- When retention policies and labels embed deletion actions, Microsoft 365 systematically processes the primary sites/accounts/mailboxes and deletes files/items. For SharePoint and OneDrive, to calculate deletion eligibility in the primary site, the file properties and metadata attributes of the top (current) version are evaluated; each version is not separately evaluated for deletion eligibility. The hidden archives are also processed and deletion eligibility is separately calculated for each version.
  - SharePoint, OneDrive and Exchange sites/accounts/mailboxes are processed at least every seven days to delete eligible content.
    - For user, shared and group mailboxes, if the query length of all applied retention policies and eDiscovery holds exceeds 10,000 characters total, mailbox deletion actions associated with eDiscovery hold cleanup tasks are not processed.
    - For Teams channel messages and Teams chats, the applied *retention policy* deletes both the regulated record in the Exchange service and the separate copy in the Azure chat service, which stores the current messages displayed in Teams.
    - Exchange public folders are not automatically processed for deletion; manual deletion is required.
  - Optionally, a *regulatory record label* can be configured to 'Trigger a disposition review,' which will:

[30] When links are shared, this is referred to as a cloud attachment.

- Review mailboxes with at least 10 megabytes of data in the mailbox.
- Send a weekly email notification to users (individuals or mail-enabled security groups) with content to review.
- Require reviewers use the disposition tab in the Microsoft 365 *compliance center* to review the content and decide whether to permanently delete it, extend its retention period, or apply a different *retention label.* NOTE: When a *regulatory record label* is applied to a file, it cannot be removed. Therefore, applying a different *retention label* is not an option for these files/items.

▶ Microsoft has discontinued the practice of automatically deleting versions that exceed the version configuration, when a *retention policy* or a *retention label* with a retain action is applied.
NOTE: A *regulatory record label* blocks the generation of a new version, after the label is applied.

▶ Deleted files and mailbox items are staged before final deletion occurs:

- In SharePoint and OneDrive, a two-stage recycle bin is utilized, which results in retaining deleted items for 30 to 93 days.
- Deleted mailbox items are kept in the hidden archive for a minimum of 14 days, which may be configured to a period up to 30 days. Additionally, calendar items deleted after they are eligible are retained for 120 days.

▶ User and lifecycle actions to delete a SharePoint site or OneDrive account are blocked, until all associated files are deleted.

▶ When a *retention policy* or *eDiscovery hold* is applied to an Exchange mailbox it cannot be deleted and instead is automatically designated as *inactive*. (See subsection *5. Special Handling,* for additional information.)

5. Special Handling

▶ Multiple features (e.g., a *regulatory record label, retention policy(ies)* and *eDiscovery hold(s))* may apply to a file or electronic mail message.

- The retention period of the *regulatory record label* is honored in primary site/account/mailbox. (See subsection *2. Regulatory Record Labels,* above.)
- Thereafter, the record is retained in either the site/account/mailbox or the hidden archive until all applicable retention and hold requirements (e.g., *retention policies* and *eDiscovery holds)* have expired.
- As a reminder, Teams setup creates both a (1) group mailbox and (2) connected SharePoint site.
  - A *retention policy* must be applied to the group, if the group mailbox contains email messages required for regulatory compliance. NOTE: Users are unable to apply *retention labels,* including *regulatory record labels* to items in group mailboxes.
  - When assigned, the *retention policy* is automatically applied to both the (1) group mailbox and (2) connected SharePoint site.
  - ♦ Additionally, *retention labels,* including *regulatory record labels,* may be published to SharePoint sites, including group connected sites. In these cases, a combination of a *regulatory record label* and *retention policies* may apply to a SharePoint file.

- When a *retention policy* with *preservation lock* or a *regulatory record label* requires records to be retained, the following protections apply:
  - The site/account/mailbox and its hidden archive is retained until all files/items are eligible for deletion.
  - New *retention policies* and *eDiscovery holds* can be applied to (a) SharePoint sites and OneDrive accounts, regardless of status and (b) active and inactive user, shared or group mailboxes.
  - Point-in-time *restores* of a SharePoint site or OneDrive account are blocked.
  - User and lifecycle processes to delete an Exchange user, shared or group mailbox results in marking the mailbox as *inactive,* rather than being deleted.
    - The *inactive* mailbox continues to be processed (eligible items are deleted), in accordance with the *retention policies, retention labels* and *eDiscovery holds* that were applied before it became inactive.
      - Since users no longer have access to an *inactive* mailbox, if items should expire, a retention feature with a delete action must be applied to the mailbox to automate deletion.

- An *inactive* user, shared or group mailbox may be *restored,*[37] to provide access to the contents of the *inactive* mailbox, including archived Skype for Business, Teams channel messages or Teams chats.
  - An *inactive* user, shared or group mailbox may be *recovered*.[32] The recovery process will apply the *retention policies, retention labels* and *eDiscovery holds* from the inactive mailbox to the items copied to the new mailbox.
  - An *inactive* mailbox, when configured with an auto-expanding archive, cannot be *recovered* or *restored*. Instead, content search tools may be leveraged to export the mailbox items and then import them to another mailbox, without altering the contents of the *inactive* mailbox.
  - For the Microsoft 365 Exchange service, the HoldCleanup parameter may be used to remove duplicate versions of mailbox items from the hidden archive. An administrator may run this command in scenarios where the hidden archive exceeds its storage limit. This command is often used in scenarios where duplicate versions of calendar items are saved due to Outlook synchronization issues.

- Reactions (e.g., likes/thumbs up) applied to Teams channel messages, Teams chats or electronic mail messages are not retained in the Exchange mailbox.
  - For Teams channel messages and/or Teams chats, applying and removing reactions is tracked in the Microsoft 365 unified audit system. To retain these reactions for regulatory compliance, the regulated entities must (a) export the audit activities to a file and store the exported file in a compliant solution for the required retention period and (b) assure that the source message has appropriate retention and compliance controls applied to it.
  - For electronic mail messages, features are not yet available to capture and store reactions for regulatory compliance.

[31] The **restore** process copies and merges the contents of the *inactive* mailbox into an existing mailbox, while continuing to preserve the inactive mailbox as is, with the applied governance policies.

[32] The **recovery** process converts the mailbox contents to a new mailbox; and thereafter, the inactive mailbox no longer exists.

2.1.3.3 *Legal Holds*

- eDiscovery holds may be applied to preserve records required for litigation, subpoena and other similar circumstances and should be removed when the matter is resolved.
  - When an *eDiscovery hold* is applied to a record, before the record is updated, a copy of the record is added to the hidden archive, where it is retained until both (a) applied *retention policies* expire (the longest *retention policy* wins) and (b) *eDiscovery holds* are removed.
  - If the record is **deleted** (by a user or by a lifecycle action), the record is retained in a hidden archive until both (a) applied *retention policies* (the longest *retention policy* wins) and (b) *eDiscovery holds* are removed.
- An *eDiscovery hold created and accessed from the compliance center* preserves records subject to the Hold. A legal case must be created. Advanced search criteria may then be entered to locate relevant content in one or more of the assessed Microsoft 365 services. For full-text queries, the first and top (current) version in a SharePoint and OneDrive document library and all versions in the hidden archive, are searched. The records that meet the query terms are associated with the selected case and are preserved indefinitely by the *eDiscovery hold* feature. Results can be exported for further analysis.
- There is no limit to the number of *cases* allowed for an organization, however, limits apply to the number of allowed *eDiscovery holds* per organization, and the number of Exchange mailboxes, SharePoint sites, and OneDrive sites per *eDiscovery hold.*
- When the legal hold is resolved, the associated *eDiscovery hold* should be removed, at which time, preservation control will be returned to other applied *retention policies* and *retention labels.*

2.1.3.4 *Clock Management*

- The Microsoft 365 Exchange service servers use the Windows Time Service to synchronize the clocks of servers on the network.
  - Although the Windows Time Service is not an exact implementation of the Network Time Protocol (NTP), it uses a complex suite of algorithms and the NTP to help synchronize time across a network. NTP is an Internet time protocol that includes the discipline algorithms necessary for synchronizing clocks.
  - Microsoft and client administrators are not authorized to change the time used by the Microsoft 365 Exchange service servers.
- SharePoint and OneDrive use Azure Blob storage, which utilizes geographically dispersed, NTP Stratum 1time servers, synchronized with Global Positioning System (GPS) satellites, as its authoritative time source.
  - Azure datacenter routers are continually synchronized with this authoritative time source.
    - Microsoft and client administrators do <u>not</u> have permissions to change the time on the data center routers.
  - All Azure domain servers and network devices, in turn, synchronize time with the data center routers. These systems are continuously conditioning by slowing or accelerating the speed of the clock, as necessary, to adjust to the authoritative GPS time.
  - Several Azure services monitor expired time; therefore, if the system time were to become out of synch by an amount in excess of the defined limits, certain Azure services would no longer function; and, manual intervention would be required.

- Only highly privileged Microsoft system administrators with the Primary Domain Controller (PDC) emulator role for the domain are allowed to change the time of the Azure domain servers and network devices. This role is very limited.

2.1.3.5 Security

- A Role Based Access Control (RBAC) permissions model is used to create a Role Group (set of roles) and then to assign individual users or user groups to a Role Group.
- Multiple layers of security protect Microsoft 365, including physical data center security, network security, access security, application security, and data security. Microsoft 365 undergoes rigorous, third-party audits of security, privacy and compliance controls on a regular basis.
- Data at rest is encrypted on servers that store records.
  - Optionally, using the customer key service, the regulated entity may configure Microsoft 365 to utilize an encryption key that it defines to encrypt data at rest.
  - When a customer key service is not applied, encryption policies controlled and managed by Microsoft will be utilized.
- Customer data in transit through Microsoft 365 services is secured using TLS/SSL communications security protocol.

2. 1.4 Additional Considerations

For Microsoft 365 services that retain regulated records for compliance with the Rule, the regulated entity is responsible for:

- Understanding where regulated records are retained, which may include: (a) user, shared or group mailboxes in Exchange; (b) Exchange public folders; (c) Skype for Business, Teams channel messages and Teams chats archived into hidden folders in Exchange, (d) SharePoint document libraries, and (e) OneDrive document libraries. See Section 1.3, *Microsoft 365 Overview and Assessment Scope,* for additional details.
  - Establishing procedures and monitoring to ensure that records for regulatory compliance are created and maintained only in locations that support compliance.
  - Understanding when records are stored in the primary site/account/mailbox versus the hidden archive and the application of compliance retention features. For example, full-text search, using *eDiscovery search,* queries the first and top (current) version in a SharePoint and OneDrive document library and all versions in the hidden archive.
  - Assuring Microsoft 365 features/services that are not compliant with the Rule are systematically disabled or procedurally disallowed (with monitoring, if needed) for retention of regulated records. Examples of non-compliant features/services include private channels, lists in SharePoint and OneDrive, and reactions in Outlook; see Section 1.3, *Microsoft 365 Overview and Assessment Scope,* the types of content not stored in accordance with the Rule.)
  - Utilizing other recordkeeping solutions for regulated records *excluded* from this assessment or unable to be protected in compliance with the Rule.

  - Exporting reactions (e.g., likes/thumbs up) applied to Teams channel messages and Teams chats from the Microsoft 365 unified audit system and storing the exported file in a compliant solution for the required retention period. Additionally, assuring that the source message also has appropriate retention and compliance controls applied to it.

- Applying location-appropriate compliance features (i.e., *retention policies* with *preservation lock* or *regulatory record labels* and *label policies* with *preservation lock)* as described in Section 1.3, *Microsoft 365 Overview and Assessment Scope,* for each location intended to store regulated records.
  - Defining retention periods that meet or exceed the retention requirements established by regulators and self-regulatory organizations, e.g., FINRA.
  - Evaluating options to apply *retention policies,* with *preservation lock,* or *regulatory record labels* to regulated records within a reasonable period (e.g., 24 hours) of creating a final record.
  - Minimizing manual actions taken by users to apply compliance retention features to electronic mail messages. NOTE: *Retention policies* are automatically applied, whereas *regulatory record labels,* require manual user actions.
- Identifying the appropriate location for collaboration. Since a *regulatory record label* prohibits editing, collaboration and content development should be completed in a location that is not governed by a *regulatory record label.*
- Carefully managing versions.
  - Applying appropriate compliance retention features to files shared via a link, i.e., cloud attachments, when the shared file is required for regulatory compliance.
  - Deleting prior versions, if these drafts are not required for regulatory compliance. NOTE: If a user starts a new file by leveraging content from another file, the first version(s) will contain irrelevant content that is potentially private. For example, if a user starts a new customer complaint response by leveraging content from a similar response, the first versions may contain the original complainant's private information.
    - Options for trimming versions include:
      - ■ Using the 'File save a copy,' which generates a new file that initially has only one version.
      - Uploading a unique file to Microsoft 365, which initially has only one version. (NOTE: Moving files from another Microsoft 365 location will keep all versions.)
      - Opening the file in SharePoint or OneDrive and selecting 'Delete All Versions' from the Version History view.
    - Once the file has the correct version set, store the file in a location that inherits the appropriate *retention policy* or *regulatory record label* and confirm that the label applied.
- Training users on methods of applying and confirming the application of *regulatory record labels*. See Section 2.1.3.2., *Compliance Retention Features,* and subsection *2. Regulatory Record Labels* for important information.
- Monitoring the files in libraries, folders and document sets to assure that *regulatory record labels* are inherited, as expected.

  - Since only one label can be applied to a file at a time; if a previously applied explicit, implicit or persistent label is detected, the existing label is not overwritten.
  - File **moves** are most likely to present challenges.

- Enabling the *archiving* feature in Skype for Business for each user, with regulated records.
- Assuring that *inactive* mailboxes are properly managed, including automated deletion, as appropriate, since users do not have access to inactive mailboxes.
- Configuring Skype for Business and Teams meetings to require guests to wait in the lobby until admitted by an authenticated user; at least one member of the interaction must be logged in as an authenticated user for the Skype for Business content and Teams meeting chats to be archived. Additionally, consider applying the most restrictive *retention policy* to all users, since any authenticated user may admit guests from the lobby.
- Assuring the asset identifier is added as metadata prior to applying the *regulatory record label,* when an event-based retention period applies to the record.
- Monitoring logs and quotas to ensure storage limits are not exceeded and that sites/accounts/mailboxes and associated hidden archives are expanded as needed, keeping in mind that fees for additional storage may be incurred.
- Applying *eDiscovery holds* for records required for subpoena, litigation or other similar circumstances; or, establishing an alternative method of preserving items needed for legal matters that is outside of Microsoft 365 services.
- Maintaining appropriate licenses and paying for all appropriate services to ensure that records are retained until their retention period has expired and any *eDiscovery hold* has been removed or until the records have been transferred to another compliant solution.

2.2 Accurate Recording Process

221 Compliance Requirement [SEC 17a-4(f)(2)(ii)(B)J

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

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

222 Compliance Assessment

Cohasset upholds that the assessed capabilities of Microsoft 365 services, in conjunction with the inherent capabilities of advanced storage technology, meet this SEC requirement for accurate recording and post-recording verification.

223 *Capabilities of the Assessed Microsoft 365 Services*

Microsoft 365 services utilize advanced electronic recording technology which applies a combination of checks and balances to assure that records are written in a high quality and accurate manner.

- At the time of recording, checksums are (a) calculated to assure that the records are written in a high-quality and accurate manner and (b) stored to enable post-recording integrity verification.
- The records are written utilizing erasure coding or replication to assure durability. See Section 2.7, *Duplicate Copy of the Records Stored Separately.*
- Checksums are regularly recalculated and compared to the stored values to validate the integrity of electronic records and detect any errors.
- If an error is identified by one of these checks, the corrupt replica is discarded, and data is corrected using duplicate data.

224 *Additional Considerations*

There are no additional considerations related to this requirement.

2.3 Serialize the Original and Duplicate Units of Storage Media

231 *Compliance Requirement [SEC 17a-4(f)(2)(ii)(CJJ*

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

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

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

232 *Compliance Assessment*

Cohasset asserts that the capabilities of the assessed Microsoft 365 locations meet this SEC requirement to serialize the original and duplicate records.

233 *Capabilities of the Assessed Microsoft 365 Services*

Microsoft 365 services systematically apply and retain system-generated creation (storage) timestamp and unique identifiers, along with change keys (versions) for each record stored in the assessed Microsoft 365 locations. This serializing information is an integral part of the metadata for each duplicate/replica made for data resiliency.

- For the Exchange service, each record is assigned the following serializing data, which is stored as metadata for the original and duplicate record (i.e., replica made for data resiliency):

- System-generated dates and times: (a) creation timestamp for items created in or are archived to Exchange and (b) received timestamp for items received by Exchange, including sent items.
- Unique Item Identifier and Change Key (version), which is assigned to electronic mail messages and Teams communication segments, e.g., Teams channel messages, Teams chats and Skype for Business instant messages.

▶ For SharePoint and OneDrive document libraries, each record is assigned the following serializing data, which is stored as metadata for each original and duplicate (i.e., replica made for data resiliency) record:

- System-generated creation (storage) timestamp and last modified timestamp.
- Site Collection URL together with the system-generated file GUID (globally unique identifier) and VersionID.

▶ If a record is copied from a SharePoint or a OneDrive document library to the hidden archive, new identifiers are assigned to the copy and the *original* system-generated creation (storage) timestamp are stored as metadata for the record.

▶ The serializing metadata are stored as an integral part of the metadata for each duplicate/replica made for data resiliency.

▶ The combination of unique identifiers and system-generated dates and times serialize the records in both space and time.

2.3.4 Additional Considerations

There are no additional considerations related to this requirement.

2.4 Capacity to Download Indexes and Records

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

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

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

2.4.2 Compliance Assessment

It is Cohasset's opinion that the assessed combination of capabilities of Microsoft 365 services meet this SEC requirement to readily download indexes and regulated records, when the considerations described in Section 2.4.4 are addressed.

2.4.3 *Capabilities of the Assessed Microsoft 365 Services*

Microsoft 365 services are cloud-based and designed for high availability and site resilience. Microsoft commits to a Service Level Agreement of 99.9% that is financially-backed. Accordingly, Internet connection services are the primary equipment capacity the regulated entity needs to download indexes and records.

Using *compliance centerfeatures,* eDiscovery managers and other authorized users may initiate *content searches,* preview the results, and download the indices and records.

2.4.3.7 Exchange Content - Content Search and Export Features

- eDiscovery managers and other authorized users may search Exchange primary and in-place archive mailboxes and associated hidden archives. Search criteria includes message recipients, senders, subject, date sent or received, etc.
- Teams channel messages and Teams chats are stored and displayed in Messaging Application Programming Interface (MAPI) format. Additionally, Teams channel messages may be rethreaded as a download option.
- Emojis, giffies (GIFs), memes and stickers are stored as weblinks; the current rendition can be selected and downloaded. Optionally, these engagement features may be disabled on a per site basis.
- Reactions (e.g., likes/thumbs up) applied to Teams channel messages and Teams chats are retained in the Microsoft 365 unified audit system and are not captured as a communication in Exchange. Therefore, the reaction history cannot be reproduced with the communication. See Section 2.1.4, *Additional Considerations,* in the *Non-Rewriteable, Non-Erasable Record Format* section, for information on capturing audit activities related to reactions applied in Teams channel messages and Teams chats.
- Reactions applied to electronic mail messages are not retained in Exchange or in the unified audit system.
- The messages retained in the Microsoft 365 Exchange service may be copied to a discovery mailbox or exported to a Personal Storage Table (PST) file.
  - By default, for each downloaded item, the associated properties and metadata (index attributes) are downloaded.
  - Options when copying messages to a discovery mailbox include:
    - Enable de-duplication, which eliminates duplicates and stores only one copy of an item. NOTE: The Results log contains a row to detail every copy of a message, e.g., one user's mailbox had it in the Inbox and flagged as important, but another user's mailbox had it moved to the Deleted Items folder without reading it.
    - Include unindexed items, such as a corrupted item, a password-protected zip attachment, an audio file, or an item encrypted by a service other than Information Rights Management.
  - The download includes message content, properties and metadata (index attributes), by default.
  - The PST file, which includes the items, properties and metadata (index attributes), may be copied to a storage medium that complies with the requirements of the Rule.

2.4.3.2 SharePoint and OneDrive Document Libraries - Content Search and Export Features

- *Content search* capabilities, for eDiscovery managers and other authorized users, are robust and allow for extensive searches, as well as narrowing the search results through refined query terms.
  - Sites/accounts cannot be removed from *content search.* (Search exclusions may be applied to other search features.)
  - *Content search* queries metadata attributes for files visible to the user and files in the hidden archives. Additionally, full-text search queries extracted text from the first and top (current) version in the SharePoint and OneDrive document libraries and files/items in the hidden archives.
  - Recycle Bin content is not indexed for *content search.*
- For SharePoint and OneDrive document libraries, the results of the *content search* may be copied as native file(s) and a comma separated values (CSV) file with a column for each metadata attribute in the list.

2.4.3.3 Additional Content Search and Export Features

- Advanced eDiscovery allows organizations to collect and review linked content, including data describing when a record was created, modified, or shared from the unified audit system. Optionally, all versions of a record retained in SharePoint or OneDrive can be retrieved. Further, the exact file version that was shared as a cloud attachment (i.e., a link in an electronic mail message, Teams channel message or Teams chat) can be identified.
- Keyword searches may use Boolean logic (e.g., AND, OR, NOT), proximity operators (e.g., NEAR (n) words) and wildcards, to include or exclude specific content in the search query.
- Search conditions (e.g., date ranges, greater or less than, and contains) narrow and refine search results.
- Searches can identify SharePoint and OneDrive records that are shared with users outside of the tenant.
- Several reports document the process, including, but not limited to, an Export Summary, Manifest and Results log for each exported item, and Trace Log with details of the export process.

2.4.3.4 Encryption and Decoding Capabilities

- Microsoft manages and applies its customer key service to automatically encrypt and decrypt records.
- The regulated entity is responsible for managing and using the encryption keys that have been used in addition to the customer key service.

2.4.4 Additional Considerations

- The user conducting a *content search* is responsible for understanding where and how records are stored and for searching accordingly. For example, if a delegate sends a message on behalf of another mailbox owner, the message will be in the Sent items of the delegate.
  - Hidden archives are included in *content search.* However, associated recycle bins are not searchable.

- The stored weblinks may be used to retrieve and view the current emojis, giffies (GIFs), memes and stickers, though these weblinks may change over time. Optionally, these engagement features may be disabled on a per site basis.
- Reactions (e.g., likes/thumbs up) are not automatically captured for compliance and, therefore, are not reproduced with the Teams channel messages, Teams chats or electronic mail messages where the reaction was applied. The process to access and download reactions depends on the method used to capture and retain this information.
- Up to 24 hours delays may be experienced for the index and unified audit system to be updated and findable in searches.
- The creation (storage) timestamps are readily downloadable; however, the unique identifiers are typically downloaded only for specific files.

▶ The regulated entity is responsible for (a) maintaining its account in good standing, (b) maintaining hardware and software to access Microsoft 365 services, (c) maintaining its encryption keys that have been used in addition to the customer key service, and (d) assuring that the regulator, self-regulatory organization or designated examining authority receive downloads of the record objects and metadata (index attributes), in the requested format and medium.

2.5 Readable Projection or Production of Images for Examination

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

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

> **SEC 17a-4(f)(3)(i):** At all times have available, for examination by the staffs of the Commission and self-regulatory organizations of which it is a member, facilities for immediate, easily readable projection or production of micrographic media or electronic -storage media images and for producing e-aslly readable images

2.5.2 Compliance Assessment

Cohasset affirms the assessed Microsoft 365 services supports the regulated entity's compliance with this SEC requirement for an easily readable projection of the record objects.

2.5.3 Capabilities of the Assessed Microsoft 365 Services

▶ eDiscovery managers and other authorized users may conduct *content searches,* using the *compliance center.* See Section 2.4.3.

▶ Microsoft 365 services are cloud-based and mobile-friendly. Thus, authorized users may search for, select, open and view records using one of two types of applications:

- Web applications, which require only an Internet connection and a local computer, laptop, smartphone or other compatible device.
- Applications installed on the users' computers, laptops and other compatible devices, as part of the Microsoft 365 license agreement.

- The stored weblinks for emojis, giffies (GIFs), memes and stickers can be used to retrieve and view the current content, though these weblinks may change over time. Optionally, these engagement features may be disabled on a per site basis.
- Teams channel messages and Teams chats are stored and displayed in Messaging Application Programming Interface (MAPI) format. Additionally, Teams channel messages can be rethreaded as a download option.
- Microsoft manages and applies its customer key service to automatically encrypt and decrypt electronic records. Additionally, the regulated entity is responsible for managing and using its encryption keys.
- Both authorized users and administrators may select items and attachments (e.g., an electronic mail attachment or an embedded file) to be decrypted, opened and viewed using several services:
  - The attachment may be opened and viewed using compatible software; optionally, the attachment may be downloaded, prior to being opened and viewed.
  - An attachment *previewer* for the specific file type may be available, through the Web or another source, to render a view of the attachment.
  - Additionally, these decrypted electronic records and associated attachments may be printed.

254 Additional Considerations

See also Section 2.4.4, *Additional Considerations,* in the *Capacity to Download Indexes and Records* section.

2.6 Reproduction of Images Provided to Regulators

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

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

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

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

> ****Because SROs and state securities regulators are neither representatives nor designees of the Commission but, to the extent that they have jurisdiction over the broker-dealer*** are organizations that should have access to facsimile enlargements and download information, the Commission is proposing technical amendments to provide them with access to these records.*

262 Compliance Assessment

Cohasset asserts that the combination of capabilities of the Microsoft 365 *compliance center,* together with assessed services, support the regulated entity in meeting this requirement to provide regulators with reproductions of the record objects.

263 Capabilities of the Assessed Microsoff 365 Services

- Authorized users may search and export content, using *compliance center* (see Section 2.4.3).
- Electronic records may be decrypted, opened, viewed and printed from web applications and installed applications.
- Selected electronic records and opened attachments may be printed or copied to another compliant media, which may be provided to the regulator.

264 Additional Considerations

See also Section 2.4.4, *Additional Considerations,* in the *Capacity to Download Indexes and Records* section.

2.7 Duplicate Copy of the Records Stored Separately

2.7. 1 Compliance Requirement [SEC 17a-4(f)(3)(iii)J

SEC 17a-4(f)(3)(ifi): Store separately from the or **ginan,** a duplleate **copy of** the **record stored on** any **medium acceptable under** § **240.17a-4 lor tile time required**

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

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

2.7.2 Compliance Assessment

Cohasset upholds that the assessed capabilities of Microsoft 365 services meet this SEC requirement for a persistent duplicate copy of the record objects, by storing more than one replica of all records (including content and metadata).

2.7.3 Capabilities of the Assessed Microsoff 365 Services

Within Microsoft 365 production environments, replication results in multiple live copies of data. Standard images and scripts are used to recover lost servers, and replicated data is used to restore customer data. Administrators do not need to configure these replication services, since they are integrated into the Microsoft 365 infrastructure.

- Each Microsoft 365 Exchange mailbox is replicated across at least two, and up to four, data centers, thereby providing high availability and site resilience should software, hardware or even datacenter failures be encountered.
  - One replica is active and up to three replicas are passive.
    - The write to the active replica and at least one of the passive replicas must be complete, for a write to be finished.
    - Writes may be delayed for two passive replicas; however, if the passive replicas become too far behind, the active replica will not accept new records.

- The Microsoft 365 Exchange service continuously monitors the health of the data; and, if any error or problem is encountered, Exchange fails over to a redundant work process and one of the passive replicas becomes the active replica.
- Further, Single Item Recovery is enabled to store deleted items in the hidden archive. Deleted calendar items are stored for 120 days and other mailbox items are retained for 14 to 30 days, as configured.

▶ Duplicate copies of SharePoint and OneDrive files and metadata are created and retained to enable recovery.

- SharePoint and OneDrive store records in erasure coded segments, which are replicated.
- This assures that if an electronic record is determined to be compromised, i.e. lost or damaged, an accurate replica is restored from a duplicate or regenerated from remaining valid erasure coded segments.

2.7.4 Additional Considerations

There are no additional considerations related to this requirement.

2.8 Organization and Accuracy of Indexes

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

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

SEC 17a-4(f)(3)(iV): Organ ze and inde.x accurately all **Information ma n.tained on both** original and any **duplicate storage media**

282 Compliance Assessment

Cohasset affirms that the Microsoft 365 Exchange, SharePoint and OneDrive services meet this requirement to accurately organize and index both the original and duplicate copies.

283 Capabilities of the Assessed Microsoft 365 Services

▶ Authorized users may organize records in a folder hierarchy in Exchange user and shared mailboxes (group mailboxes do not support this capability), public folders, and SharePoint and OneDrive document libraries.

▶ Each record includes properties and metadata (index attributes) that serve as an index and permit authorized users to sort and organize the records.

▶ The accuracy of the properties and metadata (index attributes) is supported by utilizing system-generated attributes and from searching controlled data sources, such as the To, CC, BCC and From attributes for an electronic mail message, as well as author, creation (storage) timestamp for files.

▶ Additionally, *content search* queries metadata attributes for files/items in SharePoint, OneDrive, and Exchange including content that is visible to the user and also hidden archives. Full-text search queries all extracted text from emails and attachments from Exchange, the first and top (current) version from SharePoint and OneDrive document libraries, and files/items in the hidden archives.

284 Additional Considerations

The regulated entity is responsible for organizing the Microsoft 365 services and planning the folder structure to assure it is logical and aids in locating information for retrieval.

2.9 Availability of Indexes for Examination

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

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

SEC 17a-4(f)(3)(iv)(A): At all times, a member, broker, or dealer must be able to have such indexes available for examination by the staffs of the Commission and the self-regulatory organizations of which the broker or dealer is a member

2.9.2 *Compliance Assessment*

It is Cohasset's opinion that the assessed Microsoft 365 services, supports the regulated entity in meeting this SEC requirement to retrieve and export properties and metadata (index attributes).

2.9.3 *Capabilities of the Assessed Microsoft 365 Services*

- Authorized users may run *content search* (see Section 2.4.3) to find records; and then review, access and download properties and metadata (index attributes) for the selected records.
- When copying The Microsoft 365 Exchange service messages to a discovery mailbox, by default properties and metadata (index attributes) are downloaded.
- For SharePoint sites and OneDrive accounts, the properties and metadata attributes, e.g., author title, creation (storage) date, and last modified date, are downloaded, by default.

2.9.4 *Additional Considerations*

See Section 2.4.4, *Additional Considerations,* in the *Capacity to Download Indexes and Records* section.

2.10 Duplicate Copy of the Index Stored Separately

2.10.1 *Compliance Requirement [SEC 17a-4(f)(3)(iv)(B)J*

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

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

SEC 17a-4(f)(3)(iv)(B): Each index must be duplicated and the duplicate copies must be stored separately from the original copy of the index

2.10.2 *Compliance Assessment*

Cohasset asserts that the capabilities of the assessed Microsoft 365 services meet this requirement for a persistent duplicate copy of the properties and metadata (index attributes).

2.10.3 Capabilities of the Assessed Microsoft 365 Services

Within Microsoft 365 production environments, replication results in multiple live copies of data. Administrators do not need to configure these replication services, since they are integrated into the Microsoft 365 infrastructure.

- At the time of recording in the Microsoft 365 Exchange service, one or more duplicate copies of each item *and its associated properties and metadata (index attributes)* are automatically created and stored, to provide high availability and site resilience.
  - Index data is stored together with the mailbox.
  - The Microsoft 365 Exchange service continuously monitors the health of the Exchange databases, and if any error or problem is encountered, Exchange fails over to a redundant work process and one of the passive replicas becomes the active replica.
- Duplicate copies of SharePoint and OneDrive records and the associated properties and metadata (index attributes) are stored to enable error recovery.
  - An index for the entire client site is stored with failover for recovery.
  - Additionally, the properties and metadata (index attributes) are stored with the electronic records.

2.10.4 Additional Considerations

There are no additional considerations related to this requirement.

2.11 Preservation of Indexes

2.11.1 Compliance Requirement [SEC 17a-4(f)(3)(iv)(CJJ

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

SEC 17a-4(f)(3)(iv)(C): Original and duplicate indexes must be preserved for the time required for the indexed records

2.11.2 Compliance Assessment

Cohasset maintains that the assessed Microsoft 365 services meet this SEC requirement to preserve properties and metadata (index attributes) for the same retention period as the corresponding regulated records.

2. 11.3 Capabilities of the Assessed Microsoft 365 Services

- At the time of recording in Exchange service, the properties and metadata (index attributes) are simultaneously created and stored, to provide high availability and site resilience. The properties and metadata (index attributes) are retained and are deleted in conjunction with the associated record.
- In SharePoint and OneDrive, the index is stored sequentially after the record is written. The properties and metadata (index attributes) are retained for the same time period as the associated record and are deleted, upon deletion of the associated record.

2. 11.4 Additional Considerations

There are no considerations related to this requirement.

2.12 Audit System

2121 Compliance Requirement [SEC 17a-4(f)(3)(v)]

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

> **SEC 17a-4(f)(3)(v):** lhe member, broker, or **dealer must have in place an audit system providing for accountability regarding inputting of records required to be maintained and preserved pursuant to §§ 240.17a-3 and 240.17a-4 to electronic storage media and inputting of any changes made to every original and duplicate record maintained and preserved thereby**

2122 Compliance Assessment

It is Cohasset's opinion that a combination of properties and metadata (index attributes) and the Microsoft 365 unified audit system described in Section 2.12.3, when properly configured and utilized to capture and maintain audit activities, meets this requirement for accountability regarding inputting and changing regulated records, when the considerations described in Section 2.12.4 are addressed.

2123 Capabilities of the Assessed Microsoft 365 Services

- The Microsoft 365 unified audit system is enabled by default. When enabled, a default set of audit activities are automatically captured and authorized users may search the available audit activities, using the *compliance center* or Microsoft 365 Management APIs (i.e., a single extensibility platform for Microsoft 365 auditing, service communications, security, compliance and reporting). Additionally, see Section 2.14, *Preservation of Audit Results,* for the availability period of audit activities in the unified audit system.
  - The default audited activities in the unified audit system is extensive and includes, but is not limited to:
    - Creating, modifying, or deleting *retention policies, retention labels* (including *regulatory record labels)* and *label policies*.
    - Setting *preservation lock* on a *retention policy* or *label policy*.
    - Creating, modifying and deleting query-based holds and membership of eDiscovery cases.
  - For each audit activity, the following details are captured:
    - Action taken
    - User taking the action
    - Date and time of the action
    - Record/file/item identifier
- Additionally, for Exchange mailboxes, the *ApplyRecord* activity must be enabled to log activities by the mailbox administrator, delegate and owner roles to track when *'An item is labeled as a record.'* (Logging of this activity is not enabled, by default.) Once enabled, authorized users search for *ApplyRecordLabel* in the Microsoft 365 unified audit system to find these audit activities.

2124 Additional Considerations

To meet the requirements of the Rule to maintain an audit system, the regulated entity is responsible for:

- Enable audit logging of the *ApplyRecord* activity by the mailbox administrator, delegate and owner roles for Exchange mailboxes that retain records required for compliance.

- Assure the Microsoft 365 unified audit system is enabled and is never disabled, by establishing procedures and monitoring to assure it is not disabled.
  - Monitor the unified audit system to assure it captures the minimum set of audit activities to track *'inputting of records required to be maintained and preserved pursuant to§§ 240.1 la-3 and 240.1 la-4 to electronic storage media and inputting of any changes made to every original and duplicate record.'* (See Section 2.14, *Preservation of Audit Results,* for the recommended minimum list of audit activities.)
- Additionally, see Section 2.1.4, *Additional Considerations,* in the *Non-Rewriteable, Non-Erasable Record Format* section, for information on capturing audit activities related to applying and removing reactions for Teams channel messages and Teams chats. These activities are captured in the unified audit system and should be exported to a file, which is then retained on compliant media for the required retention period.

2.13 Availability of Audit System for Examination

2131 1 Compliance Requirement [SEC 17a-4(f)(3)(v)(A)]

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

SEC 17a-4(f)(3)(v)(A): At all times, a **member, broker, or dealer mus! be able to have the results of such audit system available for examination by the staffs of the Commission and the self-regulatory organizations of which the broker or dealer is a member**

2. 13.2 Compliance Assessment

It is Cohasset's opinion that the ability to (a) retrieve certain system-managed metadata attributes and (b) search and export the Microsoft 365 unified audit system supports the regulated entity's efforts to access, download, store and provide the regulator with the requested audit system data.

2. 13.3 Capabilities of the Assessed Microsoft 365 Services

- The availability of the audit activities in the Microsoft 365 unified audit system depends on (a) enabling the capture audit activities, as described in Section 2.12, *Audit System,* and (b) subscribing to Microsoft services which set an appropriate retention period or downloading the audit activities and retaining in a separate system, as described in Section 2.14, *Preservation of Audit Results.*
- During the subscribed availability period, authorized users may search, retrieve and export audit activities from the Microsoft 365 unified audit system using the *compliance center* or using the Microsoft 365 Management APIs.
- The regulated entity must provide the examiner with the requested audit activities.

2. 13.4 Additional Considerations

The regulated entity is responsible for (a) assuring the Microsoft 365 unified audit system is enabled, as described in Section 2.12, *Audit System,* (b) retaining the audit activities, as described in Section 2.14, *Preservation of Audit Results,* (c) conducting searches to locate requested audit activities, (d) printing, downloading or otherwise producing audit activities, in the requested format and medium, and (e) providing the produced audit activities to the regulator, self-regulatory organization or designated examining authority.

2.14 Preservation of Audit Results

2.14.1 Compliance Requirement [SEC 17a-4(f)(3)(v)(B)J

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

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

2.14.2 Compliance Assessment

Cohasset asserts that enabling the Microsoft 365 unified audit system, as described in Section 2.12, *Audit System,* supports efforts to meet this SEC requirement to retain the audit activities (audit results) for the same time period as the audited records. The determination of relying solely on the Microsoft 365 unified audit system depends on (a) the retention period applied to the unified audit activities, as described in Section 2.14.3, below, and (b) the retention period applied to the corresponding records.

2.14.3 Capabilities of the Assessed Microsoft 365 Services

- The Microsoft 365 unified audit system is enabled by default and must remain enabled; accordingly, the regulated entity must enact procedures and monitoring to assure that it is not disabled by a system administrator. See Section 2.12.4, *Additional Considerations,* in the *Audit System* section.
- The availability period for the unified audit activities is a minimum of 90 days; and, regulated entities may subscribe to optional services to preserve audited activities for up to 10 years.
- When audit activities are needed longer than the period retained in the unified audit system, during the availability period, authorized users must retrieve and export the audit activities required for compliance with the Rule, using the *compliance center* or using the Microsoft 365 Management APIs. The following table lists the minimum set of audit activities that must be exported and retained in the separate audit system.

Action Member Name	Description
Retention policy ana reteritioolallelactivitiesl	
NewRetentionCompliancePolicy	Administrator created a new retention policy.
SetRetentionCompliancePolicy	Administrator updated an existing a retention policy. Updates that trigger this event include adding or excluding content locations that the retention policy is applied to.
RemoveRetentionCompliancePolicy	Administrator deleted a retention policy.
NewRetentionComplianceRule	Administrator configured the retention settings for a new retention policy. Retention settings include how long items are retained, and what happens to items when the retention period expires (such as deleting items, retaining items, or retaining and then deleting them). This activity also corresponds to running the New-RetentionComQlianceRule cmdlet.
SetRetentionComplianceRule	Administrator changed the retention settings for an existing retention policy. Retention settings include how long items are retained, and what happens to items when the retention period expires (such as deleting items, retaining items, or retaining and then deleting them). This activity also corresponds to running the Set-RetentionComQlianceRule cmdlet.
RemoveRetentionComplianceRule	Administrator deleted the configuration settings of a retention policy. Most likely, this activity is logged when an administrator deletes a retention policy or runs the Remove-RetentionComQlianceRule cmdlet.
NewComplianceTag	Administrator created a new retention label.
SetComplianceTag	Administrator updated an existing retention label.
RemoveCompl ianceTag	Administrator deleted a retention label.

Action Member Name	Description
SetRestrictiveRetentionUI	Administrator ran the Set-RegulatoryComplianceUI cmdlet so that an administrator can then select the UI configuration option for a retention label to mark content as a regulatory record.
Exchange mailbox activities	
Create	An item is created in the Calendar, Contacts, Notes, or Tasks folder in the mailbox. For example, a new meeting request is created. Creating, sending, or receiving a message isn't audited. Also, creating a mailbox folder is not audited.
SendAs	A message was sent using the SendAs permission. This means that another user sent the message as though it came from the mailbox owner.
SendOnBehalf	A message was sent using the SendOnBehalf permission. This means that another user sent the message on behalf of the mailbox owner. The message indicates to the recipient who the message was sent on behalf of and who actually sent the message.
ApplyRecord Label	A message was classified as a record. This occurs when a retention label that classifies content as a record is manually or automatically applied to a message.
Update	A message or its properties was changed.
Move	A message was moved to another folder.
MoveToDeletedItems	A message was deleted and moved to the Deleted Items folder.
HardDelete	A message was purged from the Recoverable Items folder (permanently deleted from the mailbox).
Team activities]	
MemberAdded	A team owner adds members to a team, channel, or group chat.
MemberRemoved	A team owner removes members from a team, channel, or group chat.
File and page activities for SharePoint Online and OneDrive	
ComplianceSettingChanged	A retention label was applied to or removed from a document. This event is triggered when a retention label is manually or automatically applied to a message.
FileDeleted	User deletes a document from a site.
FileModified	User or system account modifies the content or properties of a document on a site.
FileModifiedExtended	This is related to the "Modified file" (FileModified) activity. A FileModifiedExtended event is logged when the same person continually modifies a file for an extended period (up to 3 hours). The purpose of logging FileModifiedExtended events is to reduce the number of FileModified events that are logged when a file is continually modified. This helps reduce the noise of multiple FileModified records for what is essentially the same user activity, and lets you focus on the initial (and more important) FileModified event.
FileMoved	User moves a document from its current location on a site to a new location.
FileRestored	User restores a document from the recycle bin of a site.
FileUploaded	User uploads a document to a folder on a site.
FileDeleted	User deletes a document from a site.
FileDeletedFirstStageRecycleBin	User deletes a file from the recycle bin of a site.
FileDeletedSecondStageRecycleBin	User deletes a file from the second-stage recycle bin of a site.
FileVersionsAllMinorsRecycled	User deletes all minor versions from the version history of a file. The deleted versions are moved to the site's recycle bin.
FileVersionsAllRecycled	User deletes all versions from the version history of a file. The deleted versions are moved to the site's recycle bin.
FileVersionRecycled	User deletes a version from the version history of a file. The deleted version is moved to the site's recycle bin.
ComplianceRecordDelete	A document that was marked as a record was deleted. A document is considered a record when a retention label that marks content as a record is applied to the document.

Action Member Name	Description
LockRecord	The record status of a retention label that classifies a document as a record was locked. This means the document can't be modified or deleted. Only users assigned at least the contributor permission for a site can change the record status of a document.
UnlockRecord	The record status of a retention label that classifies a document as a record was unlocked. This means that the document can be modified or deleted. Only users assigned at least the contributor permission for a site can change the record status of a document.
eDiscovery activities'	
HoldCreated	A query-based hold associated with an eDiscovery case was created.
HoldUpdated	A query-based hold associated with an eDiscovery case was changed. Possible changes include editing the query or date range for a query-based hold.
HoldRemoved	A query-based hold associated with an eDiscovery case was deleted. Removing the query from the hold is often the result of deleting a hold. When a hold or a hold query is deleted, the content locations that were on hold are released.
CaseMemberAdded	A user was added as a member of an eDiscovery case. As a member of a case, a user can perform various case-related tasks depending on whether they have been assigned the necessary permissions.
CaseMemberUpdated	The membership list of an eDiscovery case was changed. This activity is logged when all members are replaced with a group of new users. If a single member is added or removed, CaseMemberAdded or CaseMemberRemoved operation is logged.
CaseMemberRemoved	A user was removed as a member of an eDiscovery case.

2144 4 Additional Considerations

The regulated entity is responsible for either (a) assuring the availability period for its subscription retains audit activities in the Microsoft 365 unified audit system for required retention period or (b) exporting and storing required audit activities in a security information event management tool or other solution for the required retention period.

2.15 90-Day Notification and Compliance Representation

2151 1 Compliance Requirement [SEC 17a-4(f)(2)(i)J

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

SEC 17a-4(f)(2)(i): The member, broker, or deale.r must notify its examining authority designated pursuant to section 17(d) of the Act (15 U.S.C. 78q(d)) prior to employing electronic storage media. If employing any electronic storage media other than optical disk technolog,y(including CO-ROM), the member, broker, or dealer must notify Its designated examining authority at least 90 days prior to employing such storage media. In either case, tlie member, broker, or dealer must provide 1ts own represe11tatio11or one from the storage medium vendor or other third party with appropriate expertise thai the selected storage media meets the conditions set forth in this paragraph (f)(2)

2. 15.2 Compliance Assessment

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

2. 15.3 Capabilities of the Assessed Microsoft 365 Services

- The regulated entity is responsible for notifying its designated examining authority at least 90 days prior to employing electronic storage media, other than optical disk technology, as required by this SEC Rule.
- While submission of the notification is the responsibility of the regulated entity, (a) this Assessment Report and other documentation may be provided to the regulated entity for preparation of its notification letter or (b) Microsoft may be asked to provide the letter of representation, which may be used for the filing.

2.15.4 Additional Considerations

There are no additional considerations related to this requirement.

2.16 Availability of Information to Access Records and Indexes or Escrow

2. 16.1 Compliance Requirement [SEC 17a-4(f)(3)(vi)]

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

SEC 17a-4(f)(3)(vi): The member, broker, **or dealer must maintaln , keep current, and provide promptly upon request by the staffs of the Commission or any self-regulatory organizations of which the rnember, broker, or broker-dealer is a member all information necessary to access records and ndexes stored on the electronic storage media: or place in escrow and keep current a copy of the physical and logical file format of the electronic storage media, the field format of all different information types written 011 the electronic storage media and the source code, together with the appropriate documentatron and information necessary to access records and indexes**

2. 16.2 Compliance Assessment

Cohasset asserts that Microsoft meets this SEC requirement to maintain current information needed to access the electronic records and associated properties and metadata (index attributes).

2. 16.3 Capabilities of the Assessed Microsoft 365 Services

- Microsoft 365 is a cloud-based service, with the data stored in Microsoft data centers. Microsoft maintains the infrastructure necessary for authorized users to access the records and associated properties and metadata (index attributes).
- Through TechNet articles, biogs and other resources, Microsoft publishes readily available documentation on the features of Microsoft 365, including methods of accessing records and associated properties and metadata (index attributes).
- Administration of the solution is jointly shared by Microsoft and client administrators. In this context, Cohasset believes the Microsoft system administrators can provide the materials and support necessary for meeting this requirement of the Rule.
- Microsoft manages and applies its customer key service to automatically encrypt and decrypt electronic records.

2. 16.4 Additional Considerations

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

In the event that Microsoft no longer provides access to the Microsoft 365 cloud-based system, Microsoft will provide a method for customers to retrieve and transfer their data, as documented in Microsoft's Terms of Service and/or the customer's specific contract terms.

2.17 Designated Third Party Requirement

2. 17.1 Compliance Requirement [SEC 17a-4(f)(3)(vii)J

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

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

2. 17.2 Compliance Assessment

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

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

> *The undersigned hereby undertakes to furnish promptly to the* U.S. *Securities and Exchange Commission ("Commission") its designees or representatives, any self-regulatory organization of which it* is a *member. or any State securities regulator havTng]urisdiction over the member, broker or dealer, upon reasonable request, such Information* as *deemed necessary by the staffs of the* Commission, *any self-regulatory organization of which it ls* a *member. or any State securities regulator having jun·sdiction over the member, broker* or *dealer to download information kept on the member's, brokers or dealer's electronic storage media to .any medium acceptable under§ 240.1 la-4. Furthermore, the undersigned hereby undertakes to take reasonable steps to provide access to Information contained on the member's, broker's or dealer's electronic storage media, including,* as *appropriate, arrangements for the downloading of any record required to be maintained and preserved by the member, broker or dealer pursuant to §§ 240.1 la-3 and 240.17a,4 in* a *format acceptable to the staffs of the Commission, any self-regulatory organization of which it is a member, or any State securffies regulator having jurisdiction over the member, broker or dealer. Such arrangements will provide specifically that in the event of a fa/Jure on the part of a member, broker or dealer* to *download the record into* a *readable format and*

2. 17.3 Capabilities of the Assessed Microsoft 365 Services

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

2. 17.4 Additional Considerations

There are no additional considerations related to this requirement.

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

The objective of this section is to document Cohasset's assessment of the capabilities of Microsoft 365, as described in Section 1.3, *Microsoft 365 Overview and Assessment Scope,* in comparison to the CFTC requirements.

The individual relevant requirements cited in Section 2, *Assessment of Compliance with SEC Rule 7la-4({),* are based on the wording in SEC Rule 17a-4(f) and Cohasset's interpretation of the requirements, given the associated SEC Interpretive Releases. Specifically, the SEC's 2003 Interpretive Release reiterates that the Rule sets forth standards that the electronic storage media must satisfy to be considered an acceptable method of storage under SEC Rule 17a-4:

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

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

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

When comparing the capabilities of Microsoft 365 that align with the SEC requirements to the *principles-based* CFTC requirements, it is essential to recognize that the SEC Rule separately describes requirements for index data and an audit system, whereas the CFTC in 17 CFR § 1.31(a) establishes an expanded definition of an electronic regulatory record to include the information as specified in paragraph (i) and (ii) below.

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

The focus of Cohasset's assessment, presented in Section 2, pertains to Microsoft 365 with highly restricted features: (a) *retention policies* with *preservation lock* and (b) *regulatory record labels* published in *label policies* with *preservation lock*. These assure that the storage solution applies integrated control codes 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 these highly restricted capabilities of Microsoft 365 to the *principles-based* CFTC requirements on the *form and manner of retention* and the *inspection and production of regulatory records.*

In addition, Cohasset contends that Microsoft 365 with less restrictive configurations meets these *principles-based* CFTC requirements, when the regulated entity applies appropriate procedural controls to oversee operations that may allow content to be modified or deleted prior to expiration of the retention period. These less restrictive configurations include:

- *Retention policies* (without *preservation lock),*
- *Record labels (i.e., retention labels* with *classify as a record),* which are less restrictive than the *regulatory record labels,* and
- *Label policies* (without *preservation lock).*

These less restrictive governance features provide flexibility to remove or shorten retention periods, which may be beneficial for compliance with privacy and data protection requirements.

The table below lists the *principles-based* CFTC requirements related to the *form and manner of retention* and the *inspection and production of regulatory records.* The middle column provides Cohasset's analysis and opinion regarding the ability of the assessed Microsoft 365 services to meet the requirements for electronic regulatory records in CFTC Rule 1.31(c)-(d). In addition, for ease of reference the right-hand column lists the correlated SEC requirements described in Section 2 of this Assessment Report.

CFTC 1.31(c)-(d) Requirement	Compliance Assessment Relative to CFTC 1.31(c)-(d)	SEC 17a-4(f) Requirements Listed in the Referenced Sections
(c) Form and manner of retention. Unless specified elsewhere in the Act or Commission regulations in this chapter, all regulatory records must be created and retained by a records entity in accordance with the following requirements: (1) **Generally.** Each records entity shall retain regulatory records in a form and manner that ensures the *authenticity and reliability* of such regulatory records in accordance with the Act and Commission regulations in this chapter. (2) **Electronic regulatory records.** Each records entity maintaining electronic regulatory records shall establish appropriate systems and controls that ensure the *authenticity and reliability* of electronic regulatory records, including, without limitation: (i) Systems that *maintain* the security, signature, and data as necessary to ensure the *authenticity* of the information contained in electronic regulatory records and to monitor compliance with the Act and Commission regulations in this chapter;	It is Cohasset's opinion that the assessed capabilities of Microsoft 365, as described in Sections 2.1 through 2.4, meet CFTC requirements (c)(1) and (c)(2)(i) for electronic records. Additionally, for *records stored electronically*, the CFTC has expanded the definition of *regulatory records* in 17 CFR § 1.31(a) to include metadata: *Regulatory records means all books and records required to be kept by the Act or Commission regulations in this chapter, including any record of any correction or other amendment to such books and records, provided that, with resQ.ect to such books and records stored electronically, regulatory records shall also include:* *01 Any data necessary to access, search, or disQ.lay any such books and records: and* *UiJ All data woduced and stored electronically describing how and when such books and records were created, formatted, or modified.* [emphasis added] It is Cohasset's opinion that the assessed Microsoft 365 services retain properties and metadata (index attributes) as an integral part of the electronic record; therefore, these attributes are subject to the same retention protections as the associated electronic record. • Immutable properties and metadata (index attributes), include but are not limited to, the unique identifier, creation (storage) timestamp. For Exchange, the To, CC, BCC and From attributes and subject are also immutable. • Mutable (changeable) properties and metadata (index attributes), include last modified date, attributes for event-based retention, and file name. See Sections 2.8 and 2.11 for the assessed capabilities of Microsoft 365 services related to the authenticity and reliability of **indexes**. The Microsoft 365 unified audit system (a) retains audit activities for the retention period defined by the associated subscription and (b) exports audit activities for retention in a separate system. See Sections 2.12 through 2.14 for capabilities related to the authenticity and reliability of the audit system.	**Section 2.1 *Non-Rewriteable, Non-Erasable Record Format*** *Preserve the records exclusively in a non-rewriteable, non-erasable format* **Section 2.2 *Accurate Recording Process*** *Verify automatically the quality and accuracy of the storage media recording process* **Section 2.3 Serialize the Original and Duplicate Storage Media** *Serialize the original and, if applicable, duplicate units of storage media, and time-date for the required period of retention the information placed on such electronic storage media* ***Section 2.4 Capacity to Download Indexes and Records*** *Have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable under this paragrapmas required by the Commission or the self-regulatory organizations of which the member, broker, or dealer is a member* ***Section 2.8 Organization and Accuracy of Indexes*** *Organize and index accurately all information maintained on both original and any duplicate storage media* ***Section 2.11 Preservation of Indexes*** *Original and duplicate indexes must be preserved for the time required for the indexed records* ***Section 2.12 Audit System*** *The member, broker, or dealer must have in place an audit system providing for accountability regarding inputting of records required to be maintained and preserved pursuant to §§240.17a-3 and 240.17a-4 to electronic storage media and inputting of any changes made to every original and duplicate record maintained and preserved thereby* ***Section 2.13 Availability of Audit System for Examination*** *At all times, a member, broker, or dealer must be able to have the results of such audit system available for examination by the staffs of the Commission and the self-regulatory organizations of which the broker or dealer is a member* ***Section 2.14 Preservation of Audit Results*** *The audit results must be preserved for the time required for the audited record*

CFTC 1.31(c)-(d) Requirement	Compliance Assessment Relative to CFTC 1.31(c)-(d)	SEC 17a-4(f) Requirements Listed in the Referenced Sections
(ii) Systems that ensure the records entity is able to produce electronic regulatory records[33] in accordance with this section, and *ensure the availabilit"i,of such regulato[Y. records in the event of an emergenct or other disruetion* of the records entity's electronic record retention systems; and	It is Cohasset's opinion that the replication and data resiliency features of the assessed Microsoft 365 services described in Sections 2.7 and 2.10 meet the CFTC requirements (c)(2)(ii) to *ensure the availabilitt of such regulato[Y. records in the event of an emergenct or other disruetion of the records entit"i,'s electronic record retention S'i_stems.*	***Section 2.7 Duplicate Copy of the Records Stored Separately*** *Store separately from the original, a duplicate copy of the record stored on any medium acceptable under §240.17a-4 for the time required* ***Section 2.10 Duplicate Copy of the Index Stored Separately*** *Each index must be duplicated and the duplicate copies must be stored separately from the original copy of each index* ***Section 2.14 Preservation of Audit Results*** *The audit results must be preserved for the time required for the audited records*
(iii) The creation and maintenance of an *UQ.-to-date inventory* that identifies and describes each system that maintains information necessary for accessing or producing electronic regulatory records.	The regulated entity is required to create and retain an *up-to-date inventory,* as required for compliance with 17 CFR § 1.31(c)(iii).	N/A
(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) *Inseection*. All regulatory records shall be open to inspection by any representative of the Commission or the United States Department of Justice. (2) *Production of **o.ao.er** regulato[Y. records.* *** (3) *Production of **electronic** regulatort 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 reaulatorv records in the form and medium*	It is Cohasset's opinion that the capabilities described in the following sections support the regulated entity's efforts to comply with the CFTC requirements for *inseection and Q.roduction of regulator'i. records stored electronicallr* Specifically, it is Cohasset's opinion that: • Sections 2.4, 2.5, and 2.6, pertain to the inspection and production of electronic records. • Sections 2.4, 2.9 and 2.11 pertain to the inspection and production of indexes. • Section 2.13 pertains to the inspection and production of the audit activities. Further, as noted in the *Additional Considerations* in Sections 2.4, 2.6, 2.9, and 2.13, the regulated entity is obligated to produce and provide the records, index and audit activities (respectively) in the form and medium requested.	***Section 2.4 Capacity to Download Indexes and Records*** *Have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable under this paragrapm as required by the Commission or the self-regulatory organizations of which the member, broker, or dealer is a member* ***Section 2.5 Readable Projection or Production of Images for Examination*** *At all times have available, for examination by the staffs of the Commission and self-regulatory organizations of which it is a member, facilities for immediate, easily readable projection or production of micrographic media or electronic storage media images and for producing easily readable images* ***Section 2.6 Reproduction of Images Provided to Regulators*** *Be ready at all times to provide, and immediately provide, any facsimile enlargement which the staffs of the Commission, any self-regulatory organization of which it is a member, or any State securities regulator having jurisdiction over the member, broker or dealer may request*

[33] 17 CFR § 1.31(a) includes indices *(Anydata necessary to access, search, or display any such books and records)* in the definition of regulatory records.

CFTC 1.31(c)-(d) Requirement	Compliance Assessment Relative to CFTC 1.31(c)-(d)	SEC 17a-4(f) Requirements Listed in the Referenced Sections
requested promptly, upon request, unless otherwise directed by the Commission representative. *(4) Production of **original** regulatoet. records.* ***		***Section 2.9 Availability of Indexes for Examination*** *At all times, a member, broker, or dealer must be able to have such indexes available for examination by the staffs of the Commission and the self-regulatory organizations of which the broker or dealer is a member* ***Section 2.11 Preservation of Indexes*** *Original and duplicate indexes must be preserved for the time required for the indexed records* ***Section 2.13 Availability of Audit System for Examination*** *At all times, a member, broker, or dealer must be able to have the results of such audit system available for examination by the staffs of the Commission and the self-regulatory organizations of which the broker or dealer is a member*

4 | Conclusions

Cohasset assessed the capabilities of certain Microsoft 365 services, in comparison to the requirements set forth in SEC Rule 17a-4(f) and its associated Interpretive Releases. This assessment includes features available through the *compliance center* along with Microsoft 365 services to store and manage electronic records in Exchange, SharePoint or OneDrive; see Section 1.3, *Microsoft 365 Overview and Assessment Scope,* for the scope and a description of included records. As of the date of this report, *only* the type of compliance retention features described for each location in the following table has been assessed for compliance with SEC Rule 17a-4(f).

***Compliance center* retention features**	**Microsoft 365 location**
Retention policy with *preservation lock*	• SharePoint site document libraries • OneDrive account document libraries • Exchange **user, shared or group** mailboxes[34] for sent and received electronic mail messages and calendar entries • Exchange public folders • Skype for Business peer-to-peer instant messaging and web conferencing transcripts, when stored in an Exchange mailbox • Teams channel messages, when stored in an Exchange mailbox • Teams chats, when stored in an Exchange mailbox
Regulatory record labels published in a *label policy* with *preservation lock*	• SharePoint site document libraries • OneDrive account document libraries • Exchange **user or shared** mailboxes for sent and received electronic mail messages only

Cohasset determined that the assessed Microsoft 365 services have the following capabilities, which meet the regulatory requirements of the Rule or support the regulated entities effort to achieve compliance:

- Capturing and retaining records in a non-erasable, non-rewriteable format by applying appropriately configured compliance retention features (see previous table), which establish integrated control codes to the storage solution to protect records from deletion, overwrite or modification, by users or lifecycle policies, prior to expiration of the associated retention period(s). In addition, using *preservation lock* provides integrated controls that *prevent* shortening the duration assigned to the *retention policy* and removing the retention controls from a record.

- Assuring immutability of the record after the retention period expires; and, preserving immutable records beyond the retention period when required by certain circumstances, such as a subpoena, litigation or legal hold, using the *eDiscovery hold* feature in the *compliance center*.

- Automatically verifying the accuracy and quality of the recording process through advanced storage technology and applying checksums during the recording process. The checksums are utilized to perform

[34] The *retention policy* with *preservation lock* applied to a group will automatically apply to the group mailbox and the connected SharePoint site. For example, Teams setup automatically creates a group mailboxes and a connected SharePoint site.

post-recording integrity verifications. When an error is detected, an accurate replica of the record is recovered or regenerated.

- Capturing the creation or receipt timestamp and creating an exclusive identifier which, in combination, uniquely serializes each record.
- Storing at least two copies of both the record and the properties and metadata (index attributes) and providing for recovery or regeneration of both the record and index information.
- Capturing properties and metadata (index attributes) for each record stored and retaining the index information for the same period of time as the record to which it pertains. In addition, authorized users can organize records in a hierarchy of folders in user and shared Exchange mailboxes, public folders, SharePoint and OneDrive. Additionally, Teams channel messages are threaded; and, Teams chats and Skype for Business conversations are organized chronologically.
- Allowing authorized users to readily sort and filter records using properties and metadata (index attributes) in Exchange mailboxes, public folders, SharePoint and OneDrive, and then download selected records, properties and metadata (index attributes) to a medium acceptable under the Rule.
- Providing authorized users with robust *content search* tools to query the properties and metadata (index attributes) stored for each record. These tools and search capabilities include full-text searches and keyword searches with a broad range of search conditions for text-based content. Audio files and video files are examples of content that is not text-based.
- Managing and using encryption policies (controlled and managed by Microsoft) and the customer key (if this service is used by the regulated entity) to encrypt and decrypt records and associated properties and metadata (index attributes).
- Generating human-readable renditions of the stored records in standard formats, except that (a) weblinks are stored for emojis, giffies (GIFs), memes and stickers and (b) the history of reactions (e.g., likes/thumbs up) applied to and removed from Teams channel messages and Teams chats are not retained by the source application and instead are tracked in the Microsoft 365 unified audit system. This requires (a) converting weblinks to the appropriate symbols, (b) exporting audit information associated with reactions to Teams Channel message and Teams chats to a file that is stored it in a compliant solution for the required retention period and (c) assuring the source message is retained for the same period as the reaction.
- Making comprehensive audit activities available in the unified audit system for to up to 10 years, depending on subscription terms; and, providing tools for the regulated entity to export audit activities, which may then be retained a separate system for the required retention period.

Accordingly, when compliance features are properly configured, carefully applied and managed, as described in this Assessment Report, it is Cohasset's opinion that the assessed Microsoft 365 services meet the non-rewriteable, non-erasable requirement by applying a combination of *retention policies* and *regulatory record labels* (with *preservation lock),* together with *eDiscovery holds* to records stored in (a) Exchange, (b) SharePoint and (c) OneDrive (see Section 1.3, *Microsoft 365 Overview and Assessment Scope).* Further, the assessed Microsoft 365 services meet or support the regulated entities' efforts to achieve compliance with the other requirements of the Rule. Additionally, Cohasset concludes that the assessed capabilities of Microsoft 365 meet the principles-based requirements of CFTC Rule 1.31(c)-(d).

5 I Overview of Relevant Regulatory Requirements

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

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

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

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

- The Rule itself, as modified over time by the SEC. These modifications to the original Rule have not affected the requirements for electronic storage media, which are the basis of this assessment. However, certain Interpretive Releases have clarified the context and meaning of certain requirements and conditions of the Rule.
- SEC Interpretive Release No. 34-44238, *Commission Guidance to Broker-Dealers on the Use of Electronic Storage Media under the Electronic Signatures in Global and National Commerce Act of 2000 with Respect to Rule 77a-4(f},* dated May 1, 2001 (the "2001 Interpretive Release").
- SEC Interpretive Release No. 34-47806, *Electronic Storage of Broker-Dealer Records,* dated May 7, 2003 (the "2003 Interpretive Release").

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

> *(f) The records required to be maintained and preserved pursuant to§§ 240. 7 la-3 and 240.1 la-4 may be immediately produced or reproduced on "micrographic media" (as defined in this section) or by means of "electronic storage media" (as defined in this section) that meet the conditions set forth in this paragraph and be maintained and preserved for the required time in that form.*
>
> *(1) For purposes of this section:*
>
> *(ii) The term electronic storage media means any digital storage medium or system and, in the case of both paragraphs (f)(7)(i) and (f)(1)(ii) of this section, that meets the applicable conditions set forth in this paragraph (f).* [emphasis added]

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

> ***SUMMARY:*** *The Securities and Exchange Commission ("Commission") is amending its broker-dealer record preservation rule to allow broker-dealers to employ, under certain conditions, electronic storage media to maintain records required to be retained. The amendments reflect a recognition of technological developments that will provide economic as well as time-saving advantages for broker-dealers bv expanding the scope of recordkeeping options while at the same time continuing to require broker-dealers to maintain records in a manner that preserves their integrity. The Commission is also issuing an interpretation of its record preservation rule relating to the treatment of electronically generated communications.*
>
> ***
>
> ***II. Description of Rule Amendments***
> ***A. Scope of Permissible Electronic***
> ***Storage Media***
>
> ****The Commission is adopting a rule todav which, instead of specifying the tvpe of storage technology that mav be used, sets forth standards that the electronic storage media must satisfy to be considered an acceptable method of storage under Rule 17a-4. Specifically, because optical tape, CD-RO/VI, and certain other methods of electronic storage are available in WOR/VI and can provide the same safeguards against data manipulation and erasure that optical disk provides, the final rule clarifies that broker-dealers may employ any electronic storage media that meets the conditions set forth in the final rule.*[35] [emphasis added]

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

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

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

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

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

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

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

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

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

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

See Section 2, *Assessment of Compliance with SEC Rule 7la-4({),* for a list of each SEC electronic records storage requirement and a description of the assessed capabilities of Microsoft 365 services related to each requirement.

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

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

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

5.3 Overview of CFTC Rule 1.31(c)-(d) Electronic Regulatory Records Requirements

Effective August 28, 2017, the Commodity Futures Trading Commission (CFTC) amended 17 CFR § 1.31 ("CFTC Rule") to define principles-based requirements for organizations electing to retain electronic regulatory records. The CFTC requirements for electronic regulatory records evolved through amendments to Rule 1.31. The most substantive changes included:

- The June 28, 1999, amendment first implemented the technical provisions regarding the use of electronic storage media for required books and records.
- The November 2, 2012, amendment clarified the retention period for certain oral communications.
- The August 28, 2017, amendments modernize and make technology-neutral the form and manner in which regulatory records, including electronic regulatory records, must be retained and produced.

To address the transition to electronic regulatory records, the CFTC amended and modernized its recordkeeping regulation to adopt principles-based standards that are less prescriptive. This resulted in rephrasing and modernizing the requirements previously defined in 1999, as explained in the August 28, 2017, Federal Register in *Ill. Final Rules, D. Regulation 7.37(c): Form and Manner of Retention:*

> *Consistent with the Commission's emphasis on a less-prescriptive, principles-based approach, proposed§ 7.37(d)(7) would rephrase the existing requirements in the form of a general standard for each records entity to retain all regulatory records in a form and manner necessary to ensure the records' and recordkeeping systems' authenticity and reliability. The Commission proposed to adopt§ 7.37(d)(2) to set forth additional controls for records entities retaining electronic regulatory records. The Commission emphasized in the Proposal that the proposed regulatory text does not create new requirements, but rather updates the existing requirements so that they are set out in a way that appropriately reflects technological advancements and changes to recordkeeping methods since the prior amendments of§ 7.37 in 7999.* [emphasis added]

The definitions established in 17 CFR § 1.31(a) are paramount to applying the CFTC requirements.

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

These definitions establish that recordkeeping obligations apply to (a) all *records entities,* without exception, and (b) all *regulatory records*. Further, for *electronic regulatory records,* paragraphs (i) and (ii) establish an expanded definition of an electronic regulatory record to include information describing data necessary to access, search and display electronic records, as well as information describing how and when such books and records were created, formatted, or modified.

The retention time periods for regulated records includes both time-based and event-based retention periods. Specifically, 17 CFR § 1.31 (b)(1)-(b)(3) states:

> ***Duration of retention.*** *Unless specified elsewhere in the Act or Commission regulations in this chapter:*
>
> *(7) 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)(7) and (b)(J)-(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)(7) or (b)(2) of this section for a period of not less than five years from the date on which the record was created.* [emphasis added]

For a list of the CFTC principles-based requirements and a summary assessment of the capabilities of the assessed Microsoft 365 services, in relation to each requirement, see Section 3, *Summary Assessment of Compliance with CFTC Rule 7.37(c)-(d).*

About Cohasset Associates, Inc.

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

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

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

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

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

For domestic and international clients, Cohasset:

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

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

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

Cohasset Associates

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

Microsoft Azure Storage

Abstract

Microsoft Azure Storage is a cloud-based service, available on the Microsoft Azure Cloud platform, which provides large-scale storage for multiple types of data, including Blobs, Files, Queues, Tables and Disks. The *Immutable Storage for Azure Blobs* feature, with the *Policy Lock* option, is designed to meet securities industry requirements for preserving records in a non-rewriteable and non-erasable format. Each Blob (record) is protected from being modified, overwritten or deleted until the required retention period has expired and any associated legal holds have been released.

In this Report, Cohasset Associates, Inc. ("Cohasset") assesses the capabilities of Microsoft Azure Storage relative to the recording, storage, and retention requirements for electronic records specified in:

- Securities and Exchange Commission (SEC) in 17 CFR § 240.17a-4(f), which regulates exchange members, brokers or dealers.
- Financial Industry Regulatory Authority (FINRA) Rule 4511(c), which defers to the format and media requirements of SEC Rule 17a-4(f).
- Commodity Futures Trading Commission (CFTC) in regulation 17 CFR § 1.31(c)-(d), which regulates commodity futures trading.

It is Cohasset's opinion that Microsoft Azure Storage, with the *Immutable Storage for Azure Blobs* feature and *Policy Lock* option, retains *time-based* Blobs (records) in a non-erasable and non-rewriteable format and meets relevant storage requirements of SEC Rule 17a-4(f), FINRA Rule 4511(c), and the principles-based requirements of CFTC Rule 1.31(c)-(d).

See Section 2 for Cohasset's detailed assessment of SEC requirements, Section 3 for a summary assessment of CFTC requirements, Section 4 for conclusions, and Section 5 for an overview of the relevant Rules.

BENEFIT FROM COHASSET'S INDUSTRY INSIGHT AND EXPERIENCE

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

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

Table of Contents

11 Introduction

The Securities and Exchange Commission (SEC) defines rigorous and explicit requirements for regulated entities[1] that elect to retain books and records[2] on electronic storage media. Additionally, effective August 28, 2077, the CFTC promulgated new principles-based requirements on the form and manner in which regulated entities retain and produce books and records, including provisions for electronic regulatory records.

Given the prevalence of electronic retention of books and records, these requirements apply to most broker-dealer and commodity futures trading firms and other organizations with similarly regulated operations.

The **Immutable Storage for Azure Blobs** *feature, with the* **Policy lock** *option, is designed to support compliance with the stringent requirements for the recording, storage and retention of regulated books and records. To evaluate its compliance capabilities with SEC and CFTC requirements, Microsoft engaged Cohasset to complete an independent and objective assessment of Microsoft Azure Storage, utilized with the Immutable Storage for Azure Blobs feature and Policy Lock option, relative to these requirements.*

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

1.1 Overview of the Regulatory Requirements

1.1.1 SEC Rule 17a-4(f) Requirements

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

> *The Commission is adopting a rule today which, instead of specifying the type of storage technology that may be used, sets forth standards that the electronic storage media must satisfy to be considered an acceptable method of storage under Rule 77a-4.* [emphasis added]

Further, the SEC issued two Interpretive Releases (No. 34-44238 on May 1, 2001, and No. 34-47806 on May 7, 2003), which pertain specifically to the electronic storage media requirements of paragraph (f).

Refer to Section 5.1, Overview of SEC Rule 17a-4(f) Electronic Records Storage Requirements, for a summary of the SEC Rule and these two Interpretive Releases.

Throughout this report, Cohasset uses the phrase *"regulated entity"* to refer to organizations required to retain records in accordance with the media requirements of the SEC, FINRA or the CFTC. Accordingly, Cohasset uses *"regulated entity"* instead of *"records entity,"* which the CFTC has defined as "any person required by the Act or Commission regulations in this chapter to keep regulatory records."

[2] Regulators use the phrase *"books and* records"to describe information about certain business transactions, customers, personnel and other administrative activities that must be retained under the Rules. Accordingly, Cohasset has used the term "Blob (record)," rather than just "object" or "blob", to consistently recognize that the object or blob is a required record.

1.1.2 FINRA Rule 4511(c) Requirements

Financial Industry Regulatory Authority (FINRA) Rule 4511(c) explicitly defers to the format and media requirements of SEC Rule 17a-4, for the books and records it requires.

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

1.1.3 CFTC Rule 1.31 Requirements

Effective August 28, 2017, 17 CFR § 1.31 (the "CFTC Rule"), the CFTC defines principles-based requirements for organizations electing to retain electronic regulatory records. These amendments modernize and establish technology-neutral requirements for the form and manner in which regulatory records must be retained and produced.

The definition of *regulatory records* in 17 CFR § 1.31(a) is essential to the CFTC's electronic recordkeeping requirements.

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

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

Refer to Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d),* which relates the CFTC principles-based requirements to the capabilities of Microsoft Azure Storage, as described in Section 2. Additionally, refer to Section 5.3, *Overview of CFTC Rule 1.31(c)-(d) Electronic Storage Requirements.*

1.2 Purpose and Approach

To obtain an independent and objective assessment of the compliance capabilities of Microsoft Azure Storage ("Azure Storage"), utilized with the *Immutable Storage for Azure Blobs* feature and *Policy Lock* option, in comparison to relevant storage-specific requirements set forth in SEC Rule 17a-4(f) and CFTC Rule 1.31(c)-(d), Microsoft engaged Cohasset Associates, Inc. ("Cohasset"). As a highly-respected consulting firm, Cohasset has recognized expertise and more than 40 years of experience with the legal, technical and operational issues associated with the records management practices of companies regulated by the SEC and the CFTC. Additional information about Cohasset is provided in the last section of this report.

Cohasset was engaged to:

- Assess the capabilities of Azure Storage, utilized with the *Immutable Storage for Azure Blobs* feature and *Policy Lock* option, in comparison to the five requirements related to recording, storage and retention of electronic records, as stipulated in SEC Rule 17a-4(f); see Section 2, *Assessment of Compliance with SEC Rule 17a-4(f);*

- Associate the principles-based requirements of CFTC Rule 1.31(c)-(d) to the assessed capabilities of Azure Storage; see Section 3, *Summary Assessment of Compliance with CFTC Rule 7.37(c)-(d);* and
- Prepare this Assessment Report, enumerating the results of its assessment.

In addition to applying the information in this Assessment Report, regulated entities must ensure that the combination *of its policies, procedures and regulatory submissions, in conjunction with the capabilities of implemented electronic recordkeeping solutions, meet all applicable requirements of SEC Rule 77a-4(f) and CFTC Rule 7.37*.

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

The Azure Cloud platform is a comprehensive set of cloud services, hosted by Microsoft, which are designed for use by developers, IT professionals and Enterprises. One service available on the Azure platform is Azure Storage, which provides large-scale storage for multiple types of data, including Blobs, Files, Queues, Tables and Disks. Azure Storage for Blobs, which is the focus of this assessment, allows customers to store large amounts of unstructured data, such as text or binary data, and access it from anywhere in the world.

The *Immutable Storage for Azure Blobs* feature with the *Policy Lock* option, is designed specifically to store Blobs (records) in compliance with SEC Rule 17a-4(f). Blobs (records) are stored in Containers. When an *Immutability Policy* (retention interval) is defined at the Container level, it applies to all Blobs (records) retained within it and it protects Blobs (records), associated system and custom metadata, in a non-rewriteable and non-erasable format, for the duration of the retention period and any assigned legal holds. When the *Immutability Policy* is locked, via the *Policy Lock* option, stringent retention controls are applied, which prevent both (a) shortening the retention interval defined for an Immutability Policy and (b) removing an Immutability Policy from the Container.

This assessment addresses Azure Storage services for Blobs *only* and the specific features that are relevant for meeting the requirements of the SEC Rule. *Note: The Disk Storage*[3] *service is implemented as a type of Blob within Azure Storage and, therefore, is included in this assessment.* This assessment excludes Azure Storage services for Files, Queues, and Tables.

[3] *Disk Storage,* one of the Azure Storage services available on the Azure Cloud platform, offers fully-managed storage for virtual machine environments.

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

This section presents Cohasset's assessment of the capabilities of Azure Storage, utilized with the Immutable Storage for Azure Blobs feature and the Policy Lock option, for compliance with the five (5) requirements related to recording, storage, and retention of electronic records, as stipulated in SEC Rule 77a-4(f).

Assessment Scope

This assessment addresses Azure Storage services for Blobs only and the specific features that are relevant for meeting the requirements of the SEC Rule. *Note: Disk storage is implemented as a type of Blob within Azure Storage and, therefore, is included in this assessment.* This assessment *excludes* Azure Storage services for Files, Queues, and Tables.

Assessment Organization

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

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

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

2.1 Non-Rewriteable, Non-Erasable Record Format

2. 1.1 Compliance Requirement [SEC 17a-4(f)(2)(ii)(A)J

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

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

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

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

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

> *Moreover, there may be circumstances (such as receipt of a subpoena) where a broker-dealer is required to maintain records beyond the retention periods specified in Rule 1la-4 or other applicable Commission rules. Accordingly, a broker-dealer must take appropriate steps to ensure that records are not deleted during periods when the regulatory retention period has lapsed but other legal requirements mandate that the records continue to be maintained, and the broker-dealer's storage system must allow records to be retained beyond the retentions periods specified in Commission rules*. [emphasis added]

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

2.1.2 *Compliance Assessment*

It is Cohasset's opinion that the current capabilities of Azure Storage, with the *Immutable Storage for Azure Blobs* feature and the *Policy Lock* option, meet this SEC requirement to retain records in non-erasable and non-rewriteable format, when (a) utilized to retain Blobs (records) that require *time-based*[4] retention, (b) an appropriate retention interval is assigned to the *Immutability Policy,* (c) the *Policy Lock* option is enabled, (d) legal holds are appropriately set to preserve all Blobs (records) in the Container for purposes of litigation and other similar circumstances, and (e) the considerations identified in Section 2.1.4 are satisfied.

2.1.3 *Azure Storage Capabilities*

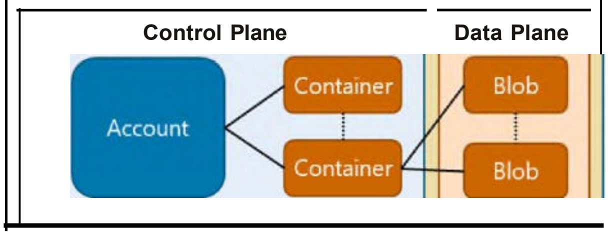
In this section, Cohasset presents the main functionality and capabilities of Azure Storage, utilized with the *Immutable Storage for Azure Blobs* feature and the *Policy Lock* option, that directly pertain to the requirement for preserving electronic record objects as non-rewritable and non-erasable, for the required retention period and any associated legal holds.

Storage Account and Container Definitions and Controls

The Azure Storage Framework consists of two conceptual components:

- **Control Plane** manages Storage Account and Container operations, including data organization, retention, and the application of immutability controls and legal hold tags.
- **Data Plane** manages data operations, such as reads, writes and deletes.

Azure Storage Framework



[4] *Time-based* retention periods require the Blob (record) to be retained for a fixed, contiguous period of time calculated from the date created/stored.

- A Subscription (client) on the Azure Cloud Platform utilizes Azure Storage Accounts, which are unique namespaces, to store and access Blobs (records).
- Containers act as virtual file folders within an Account to organize the storage of Blobs (records).
  - Container names must be unique within an Account.
  - Containers have a single-level hierarchy, meaning they cannot hold other Containers, only Blobs (records).
  - Metadata for Containers include:
    - Immutable metadata such as (a) Container name and creation/storage date/time, (b) Boolean values for the existence of an Immutability Policy and Policy Lock status (if locked), (c) Effective date/times for applied Immutability Policy, Policy Lock, and Legal Holds, (d) User IDs associated with locking the Immutability Policy, extending the policy and adding Legal Holds, and (e) prior Retention Interval and date/time that the prior Retention Interval was extended.
    - Mutable metadata such as Retention Interval, Legal Hold tags, etc.
- The *Immutable Storage for Azure Blobs* feature provides the ability to (a) apply an *Immutability Policy* (retention interval) and *Legal Holds* to a Container and (b) enable the *Policy Lock* option for the *Immutability Policy* (hereinafter *"Locked Immutability Policy")*. The *Locked Immutability Policy* and Legal Holds serve as integrated control codes, designed to preserve electronically stored Blobs (records) and associated system and custom metadata as ***non-erasable*** and ***non-rewriteable*** for the following time periods:
  - For the lifespan of the Blobs (records) when stored in a Container that is controlled by a *Locked Immutability Policy*. Note: A Blob (record) that is past retention will continue to be protected against modification and overwrites until deleted. (See *Retention - Locked Immutability Policy* subsection below, for more details.)
  - For the duration of an applied Legal Hold. (See *Legal Hold* subsection, below, for more details.)
- The following safeguards apply to Containers with a *Locked Immutability Policy* (hereinafter *"protected* Containers"):
  - The Immutability Policy (Retention Interval) cannot be deleted from the Container.
  - The Retention Interval cannot be shortened.
  - Blobs (records) cannot be deleted from the Container until the Blob's (record's) retention expiration date has passed.
- A Container cannot be deleted if it contains one or more Blobs (records) or if a Legal Hold is applied.
- A Storage Account cannot be deleted if it has one or more Containers with either a *Locked Immutability Policy* or Legal Hold applied.

Blob (Record) Definition and Controls

- Azure Storage provides storage services for three types of Blobs:

  1. Block Blobs - used to hold ordinary files up to 4.7 TB in size

     - New Block Blobs are the *only type of Blob that can be written directly to a protected Container.* Retention and immutability controls automatically apply to the new Blobs (records) as they are stored. Alternatively, new Block Blobs created outside of a protected Container can be copied to the protected Container.

  2. Page Blobs - used to hold random access files up to 8 TB in size

- Page Blobs are created outside of a protected Container, then copied to the protected Container.

  Note: Once a Page Blob is stored in a protected Container, further write operations are suspended.

  3. Append Blobs - optimized for append operations, these are typically used for logging information

     - Append Blobs, like Page Blobs, are created outside of a protected Container, then copied to the protected Container. *Note: Once an Append Blob is stored in a protected Container, further append operations are suspended.*

- A Blob (record) is comprised of:

  - Complete content of the Blob (record).

  - Immutable metadata for each Blob (record) includes:

    - System metadata, including critical attributes for record management such as Object ID (Blob name, Container name, Account name), type of Blob, creation/storage date (within Azure Storage), checksums, encryption status, etc.

    - Custom metadata at the Blob (record) level, in the form of key value pairs, may include attributes such as search index values.

  - Mutable metadata at the Blob (record) level includes:

    - The storage tier utilized to store the Blob (record). Three storage tiers exist within the Azure Storage environment:

      - Hot - utilized for Blobs (records) requiring frequent access,

      - Cool - utilized when infrequent access is required,

      - Archive - appropriate when only limited access is necessary.

      Blobs (records) may be moved between storage tiers throughout their lifespan within Azure Storage. If a *Locked Immutability Policy* has been applied to a Blob's Container, immutability controls will remain in effect for the Blob (record), regardless of which storage tier is selected, and immutable Blob (record) metadata, such as creation/storage date will remain unchanged.

- The Retention Interval is not stored as part of the metadata for each Blob (record). Rather, an Immutability Policy (Retention Interval) value, stated as the number of days to retain past the Blob's (record's) creation/storage date, is set at the Container level and is used to *calculate* the retention expiration for each Blob (record).

- To be compliant with SEC regulations, a Blob (record) must:
  - Be stored in a protected Container, and
  - Have a unique name within that Container. Azure Storage automatically prohibits Blobs (records) with a duplicate name from being saved to a protected Container.
- Once a Blob (record) is written to a protected Container, the Blob (record) is protected against (a) changes, (b) overwrites, (c) moves to any other Container, (d) snapshots, and (e) deletes, until the calculated retention expiration date has passed. Further, the Blobs (records) that are past retention will continue to be protected from changes and overwrites until deleted.
- When an *Immutability Policy* is applied to a Container, the Retention Interval and associated immutability controls apply to any *existing* Blob (record) versions already stored within the Container, however, no *new versions* are allowed for Blobs(records) within that Container.
- A Blob stored in a protected Container may be *copied* to another Container.
  - The original will remain in the original Container and be governed by the Immutability Policy and Legal Holds applied to the original Container.
  - The new copy of the Blob (record) will retain its original creation/storage date and time (when it was written to the original Container); however, its retention duration will be calculated using the Retention Interval (if any) of the new Container and any Legal Holds applied to the new Container will apply to the new copy.

Retention - Locked Immutability Policy

- For compliance with SEC Rule 17a-4(f), a *Locked Immutability Policy* must be created and applied to the Container, utilizing the following two steps:

1. The Immutability Policy (Retention Interval) is set and stored at the Container level.
   - The Retention Interval is the number of *days* that each Blob (record) stored in the Container must be retained past its creation/storage date.
   - The retention expiration date for a Blob (record) is calculated, when needed, rather than stored as Blob (record) metadata.
   - Only one Retention Interval can be assigned to each Container.
   - As soon as the Immutability Policy is applied to a Container, immutability controls are applied to Blobs (records) stored within the Container and remain in effect for the lifespan of the Blobs (records). **However, until the *Policy lock feature* is applied, the Retention Interval may continue to be modified and the Immutability Policy may be cleared (deleted). If the Immutability Policy is cleared, all immutability controls are removed from the Container.**
     - Note: Since Container operations are cached, a delay of 30 seconds or more may occur before an Immutability Policy is applied to a Container.

2. A Container's Immutability Policy ***must be locked,*** via the *Policy Lock* option, to assure:
   - The Container's Retention Interval cannot be *shortened*.
   - The Retention Interval cannot be deleted from the Container.

- Retention Intervals may be *extended* up to five (5) times per Container, up to a maximum of 400 years. If the Retention Interval is extended:
  - The new Retention Interval applies retroactively to Blobs (records) currently stored in the Container, as well as new Blobs (records) added to the Container.
  - The new Retention Interval and effective date are stored as Container metadata.
- The capabilities of Azure Storage are currently limited to time-based retention periods, i.e., records where a retention period is applied at the time of recording and is effective for a fixed, contiguous period of time. Records with event-based[5] retention requirements should be retained in a separate compliance system.

Legal Holds

- Legal Holds are set and stored at the **Container level** to preserve all Blobs (records) in the Container for purposes of subpoena, litigation, regulatory investigation, and other similar circumstances.
  - Each Legal Hold must be uniquely identified with a Legal Hold tag (Case ID) of 23 characters or less.
  - A maximum of ten Legal Holds are allowed per Container.
- All Blobs (records) stored within a tagged Container, including those written to a Container after a Legal Hold is applied, will be protected against (a) deletes, (b) changes, (c) overwrites, (d) snapshots, and (e) versioning, until all Legal Hold tags are cleared from the Container.
- A Legal Hold(s) can exist at the Container level as an independent control for the enclosed Blobs (records) and, therefore, does not require a Container to also have an assigned Immutability Policy *(locked or unlocked).*
- Legal Hold tags are removed from the Container when no longer required. If all Legal Hold tags are removed from a Container, immutability controls for the Container and Blobs (records) are governed as follows:
  - Blobs (records) stored in a protected Container will be protected against modification, overwrites and deletion for the defined retention period. Once past the retention period, Blobs (records) will continue to be protected against modification and overwrites until deleted.
  - Blobs (records) stored in a Container with no Immutability Policy are changeable, overwritable and deletable, after all Legal Holds are released.

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

Disposition/Deletion and Overwrite

- Blobs (records) and all associated metadata are protected from premature deletion and become eligible for deletion when the following conditions are met:
  - The Blob's (record's) retention expiration date, calculated by adding the Container's Retention Interval (as updated by any Retention Interval extensions) to the Blob's (record's) creation/storage date, is in the past. Note: A Blob (record) that is past retention will continue to be protected against modification and overwrites until deleted.
  - All Legal Hold tags have been cleared from the Container.
- An overwrite of a Blob (record) is only allowed when the Container holding it has (a) no assigned Immutability Policy, *either locked or unlocked,* and (b) no assigned Legal Holds.
- Deletion of a Container is prohibited if it has:
  - A *locked* Immutability Policy and/or at least one Legal Hold tag, ***and,***
  - It contains one or more Blobs (records), even if the Blobs (records) are past retention.
- Deletion of an Account that has Containers with *Locked Immutability Policies* or active Legal Holds is prohibited.

Clock Management

- Azure utilizes, geographically dispersed, NTP Stratum 1 time servers, synchronized with Global Positioning System (GPS) satellites, as its authoritative time source.
  - Azure's datacenter routers are continually synchronized with this authoritative time source.
  - All Azure domain servers and network devices, in turn, synchronize time with the data center routers. These systems are continuously conditioning by slowing or accelerating the speed of the clock, as necessary, to adjust to authoritative GPS time.
  - Several Azure services monitor expired time; therefore, if the system time were to become out of synch by an amount in excess of defined limits, certain Azure services would no longer function and manual intervention is required.
- Microsoft System Administrators and client administrators do *not* have permissions to change the time on the data center routers.
- Only highly privileged Microsoft System Administrators with the Primary Domain Controller (PDC) emulator role for the domain are allowed to change the time of the Azure domain servers and network devices. This role is very limited.

Security

- The Microsoft Azure Cloud Platform undergoes rigorous, third-party audits of security, privacy and compliance controls on a regular basis. For more information see https://azure.microsoft.com/en-us/overview/trusted-cloud/
- Encryption of Blobs (records) is available on three levels:
  - **Before transmitting to Azure Storage** - The regulated entity may use a client-side encryption service provided by Microsoft or their own encryption service to encrypt the Blobs (records).
  - **In transit to Azure Storage-** If utilizing a Microsoft VPN, all layers of the transport are secured from top layer down to physical layer via HTTPS (a secure internet transfer protocol). If transmission is done over the internet, regulated entities are encouraged to utilize HTTP Secure (HTTPS) as well.
  - **Data-at-rest on Azure Storage** - By default, data-at-rest is encrypted by Microsoft derived and managed keys. Alternatively, customers may store their own encryption keys within the Azure Key Vault, which is a hardware security module.
- Roles-based Security (RBAC) is employed at the Control Plane level. By default, Microsoft utilizes Azure Active Directory for federated identity management. Alternatively, the regulated entity may utilize their own RBAC solution.
- Access to Blobs (records) is controlled by the owner of the Azure Storage account (Super User) who can distribute Shared Access Signature (SAS) tokens. These tokens are activated for a specified period of time, during which the recipient can perform designated activities such as Read, Write or Delete. NOTE: Immutability controls established by a Container's Locked Policy or Legal Hold tag ***cannot be overridden*** by SAS tokens; only Read Access is allowed.

2.1.4 *Additional Considerations*

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

- Applying an *Immutability Policy,* with an appropriate Retention Interval, to every Container that is used to store regulated Blobs (records) and ***locking* the Immutability Policy,** either at the time the Container is created or within 24 hours of storing Blobs (records) within the Container. If Blobs (records) to be stored have multiple retention periods, the regulated entity must either (a) configure and use different Containers, each with an appropriate Retention Interval or (b) configure a single Container with a Retention Interval that is set to the longest retention period associated with the Blobs (records).
- Applying Legal Hold tags (Case IDs) to Containers with Blobs (records) that require preservation for legal matters, government investigations, external audits and other similar circumstances, and clearing the Legal Holds when the applicable action is completed.
  - Assigning descriptive, but not confidential, Legal Hold Case IDs, since the Case IDs are exposed.

- Ensuring all Blobs (records) required to be retained for compliance with the SEC Rule are uploaded to a properly configured Azure Storage Container within 24 hours of creation, or are stored in an SEC-compliant protected storage system until they are uploaded to Azure Storage.
- Establishing appropriate security policies and procedures to:
    - Restrict access to the Azure Storage Account Owner role (Super User).
    - Define the actions of the Azure Storage Account Owner.
    - Ensure appropriate levels of encryption is enabled for Blobs (records) at rest and in transit.
    - Periodically verify Microsoft's (and those of the regulated entity, where applicable) security/privacy/compliance audit results and/or certification reports.
- Ensuring that all security measures provided by a Data Trustee (in the event Sovereign Cloud Hosting is utilized) are consistent with the security measures provided by Microsoft within the Azure Storage environment.
- Storing Blobs (records) requiring event-based retention periods in a separate compliance system, since Azure Storage does *not* currently support event-based retention periods.

Further, since Legal Holds apply to *all* Blobs (records) in a Container, Cohasset also recommends that the regulated entity contemplate the type of Blobs (records) stored in each Container to limit excessive preservation of Blobs (records).

Additionally, the regulated entity is responsible for maintaining their Azure Account and Storage Subscription and paying for all appropriate services to ensure that protection of all Blobs (records) continue until their Retention Intervals have expired or until the Blobs (records) have been transferred to another compliant storage system.

2.2 Accurate Recording Process

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

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

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

2.2.2 Compliance Assessment

It is Cohasset's opinion that the use of checksums and validation processes by Azure Storage, in conjunction with the inherent capabilities of advanced electronic recording technology, meet this SEC requirement.

2.2.3 Azure Storage Capabilities

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

Recording Process

- When a Blob (record) is uploaded to Azure Storage:
  - The Blob (record) is divided into separate increments, i.e., blocks, that are written to the Azure Storage environment.
  - As blocks of data are written, Azure Storage automatically generates two secondary copies across different nodes of storage, for a total of three replicas.
  - A checksum is calculated for each block and stored as immutable metadata, at the individual block level, for post-recording verification.
  - Once Azure Storage verifies that all three replicas have been successfully written and are identical, acknowledgement of a successful write is returned to the client. If a write failure occurs at any stage, an error message is returned to the invoking application for corrective action and the write operation is stopped to prevent corrupted data from being written to Azure Storage.
  - Azure Storage then utilizes erasure coding to finalize the write, which provides an automated method of error recovery that improves data durability and optimizes the storage space utilized.
- A customer may optionally provide a check-sum with a Blob (record) during the upload process.
  - If a *block-level* checksum is provided, it will be utilized by Azure Storage to validate the recording process and will be stored as metadata.
  - If a *blob-level* checksum is provided, it will *not* be used to validate the storage process; instead, the checksum will be stored as metadata and may be accessed by the customer for independent checksum validation.
- Azure Storage 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 Blobs (records) are written in a high quality and accurate manner.

Post-Recording Verification Process

- To validate Blob (record) content, Azure Storage recalculates a checksum during every block read and compares it to the stored value calculated at the time of recording. Additionally, routine scans are run every few days to ensure recalculated checksums continue matching the stored values.
- If any block of data is determined to be corrupt, an accurate replica is recovered from a duplicate or is accurately regenerated from the erasure coded data (see Section 2.5, *Duplicate Copy of Records Stored Separately).*

2.2.4 Additional Considerations

Cohasset recommends that the regulated entity:

- Calculate and transmit checksums, at the block level, for use by Microsoft to verify the integrity of the uploaded Blob (record).
- Utilize HTTPS (a secure internet transfer protocol), if possible, when uploading Blobs (records) to reduce the chance of network-level errors.

2.3 Serialize the Original and Duplicate Units of Storage Media

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

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

SEC 17a-4(f)(2)(ii)(C): Serialize the origiraal **and. if applicable. duplfcate unfts of storage media, and fime-date for the required period of retenliora the Information placed on such electronic storage media.**

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

2.3.2 Compliance Assessment

It is Cohasset's opinion that the capabilities of Azure Storage meet this SEC requirement to serialize the original and duplicate record objects.

2.3.3 Azure Storage Capabilities

- Each Blob (record) is assigned a unique, immutable Object ID, which is exposed as a Uniform Resource Identifier (URI). The Object ID is comprised of:
  - Account name (unique per Subscriber)
  - Container name (unique per Account)
  - Blob name (unique per Container), and
  - Creation/Storage date, which is the date and time stamp when the *complete* Blob (record) content is committed to storage.
- The combination of the Account, Container and Blob name, along with the creation/storage date and time stamp, provide a serialization of each Blob (record) in both space and time.

2.3.4 Additional Considerations

There are no additional considerations related to this requirement.

2.4 Capacity to Download Indexes and Records

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

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

SEC 17a-4(f)(2)(ii)(DJ: Have the capacrty to readily download indexes and records preserved on the electronic ·storage media to any medfum acceptable under th1s paragraph (f) as required by the Commission or the self-regulatory organlzations of whfch the member, broker, or dealer is a member.

2.4.2 Compliance Assessment

It is Cohasset's opinion that Azure Storage meets this SEC requirement by providing capacity and high data availability, search services and the ability to download selected Blobs (records) and metadata (index) attributes. Downloaded Blobs (records) and metadata (index) attributes can then be transferred, by the regulated entity, in the format and media requested for production.

2.4.3 Azure Storage Capabilities

- Azure Storage capabilities that support the capacity to download Blobs (records) and associated metadata include:
  - Direct searches, via REST APIs (application programming interfaces), are allowed across the superset of system properties and metadata, e.g., Container name, Retention Interval, Policy Lock Status, Object ID (Account/Container/Blob name), creation/storage date, last modified date and user ID. Search results can be saved to a separate database or downloaded to a media of choice.
  - Azure Search is a separate Azure Cloud platform service which reads through system and custom metadata, of both Containers and Blobs (records), to create an index which can then be saved to any database, e.g., MySQL, Cosmos DB, etc.
  - Third-party search tools may be utilized to search system and custom metadata, for both Containers and Blobs (records), to create an index which can then be saved to a separate database of choice.
- Once a search has identified desired Blobs (records), REST APIs may be used to retrieve a copy for transfer to any other compliant storage media.
- Microsoft further supports access to Blobs (records) by ensuring the Azure Storage environment maintains high availability, and proper capacity, based on the storage tier selected. Published availability numbers can be found at https://azure.microsoft.com/en-us/support/legal/sla/storage/v1_3/

2.4.4 Additional Considerations

The regulated entity is responsible for (a) authorizing user access, (b) maintaining hardware and software to access Azure Storage, and (c) assuring that the regulator, self-regulatory organization or designated examining authority receive downloads of the Blobs (records) and metadata attributes in the requested format and medium.

2.5 Duplicate Copy of the Records Stored Separately

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

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

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

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

2.5.2 Compliance Assessment

Cohasset believes that Azure Storage meets this SEC requirement through the use of (a) replication within a single data center, or optionally, across multiple geographically separate data centers, and (b) erasure coding, whereby Blobs (records) are recorded in segments across multiple disks, in one or more facilities or regions. This assures that if a Blob (record) is determined to be compromised, i.e., lost or damaged, an accurate replica is restored from a duplicate or regenerated from remaining valid erasure coded segments.

2.5.3 Azure Storage Capabilities

- Azure Storage provides four options for replicating Blobs (records):

  1. **Locally Redundant Storage (LRS)** - Three copies of all data are made synchronously across separate fault and upgrade domains within a single facility. This is the default method of replication within Azure Storage.

  2. **Geo-Redundant Storage (GRS)** - Three LRS copies of the data are written synchronously to the primary data facility, then asynchronously, three more copies of the data (GRS) are written to a remote facility. The regulated entity does not have read access to the GRS data, as it exists for recovery purposes only.

  3. **Read-Access Geo-Redundant Storage (RA-GRS)** - This alternate version of GRS grants the regulated entity with read access to the data stored in the secondary data center.

  4. **Zone Redundant Storage (ZRS)** - This alternate replication option is available for Block Blobs only. Data is replicated synchronously across two to three *facilities,* within a single region or across two separate regions. This type of geographically separate replication offers more durability than LRS.

- After a Blob (record) has been successfully written to storage with one of the above replication methods, Azure Storage then utilizes erasure coding to optimize the storage space utilized, rather than continue to store three full replicas. Erasure coding stores segments of the Blob (record) across multiple disks, in one or more facilities or regions (depending on the replication method selected). This assures that a replica can be accurately regenerated from the erasure coded data should an error occur in one segment of the data, or should an availability problem be encountered in any one of the facilities or regions.

2.5.4 Additional Considerations

There are no additional considerations related to this requirement.

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

The objective of this section is to document Cohasset's assessment of the capabilities of Azure Storage, when utilized with the *Immutable Storage for Azure Blobs* feature and the *Policy Lock* option, in comparison to the CFTC requirements.

The individual relevant requirements cited in Section 2, *Assessment of Compliance with SEC Rule 7la-4({),* are based on the wording in SEC Rule 17a-4(f) and Cohasset's interpretation of the requirements, given the associated SEC Interpretive Releases. Specifically, the SEC's 2003 Interpretive Release reiterates that the Rule sets forth standards that the electronic storage media must satisfy to be considered an acceptable method of storage under Rule 17a-4:

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

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

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

When comparing Azure Storage capabilities that align with the SEC requirements to the *principles-based* CFTC requirements, it is essential to recognize that the SEC Rule separately describes requirements for index data and audit trail, whereas the CFTC in 17 CFR § 1.31(a) establishes an expanded definition of an *electronic regulatory record* to include the information as specified in paragraph (i) and (ii) below.

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

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

CFTC 1.31(c)-(d) Requirement	Compliance Assessment Relative to CFTC 1.31(c)-(d)	SEC 17a-4(f) Requirements Listed in the Referenced Sections
(c) Form and manner of retention. Unless specified elsewhere in the Act or Commission regulations in this chapter, all regulatory records must be created and retained by a records entity in accordance with the following requirements: (1) **Generally.** Each records entity shall retain regulatory records in a form and manner that ensures the *authenticity and reliability* of such regulatory records in accordance with the Act and Commission regulations in this chapter. (2) **Electronic regulatory records.** Each records entity maintaining electronic regulatory records shall establish appropriate systems and controls that ensure the *authenticity and reliability* of electronic regulatory records, including, without limitation: (i) Systems that *maintain* the security, signature, and data as necessary to ensure the *authenticity* of the information contained in electronic regulatory records and to monitor compliance with the Act and Commission regulations in this chapter;	It is Cohasset's opinion that Azure Storage capabilities, utilized with the *Immutable Storage for Azure Blobs* feature and the *Policy Lock* option, as described in Sections 2.1 through 2.4 meet CFTC requirements (c)(1) and (c)(2)(i) for Blobs (records). Additionally, for *records stored electronically.* the CFTC has expanded the definition of *regulatory records* in 17 CFR § 1.31(a) to include metadata: *Regulatory records means all books and records required to be kept by the Act or Commission regulations in this chapter, including any record of any correction or other amendment to such books and records, provided that, with resQ.ect to such books and records stored electronically, regulatory records shall also include:* *U) Any data necessary to access, search, or disQ.lay anv such books and records; and* *Ui! All data Q.roduced and stored electronically describing how and when such books and records were created, formatted, or modified.* [emphasis added] • It is Cohasset's opinion that Azure Storage retains immutable metadata attributes (e.g., Object ID, create date/time and Retention Interval), as an integral part of either (a) the record object itself; or (b) its Container. The Blob (record) attributes are subject to the same retention protections as the associated Blob (record) itself. • To satisfy this requirement for other essential data related to how and when the Blobs (records) were created, formatted, or modified, the regulated entity must retain this data in a compliant manner.	**Section 2.1** ***Non-Rewriteable, Non-Erasable Record Format*** *Preserve the records exclusively in a non-rewriteable, non-erasable format.* [SEC 17a-4(f)(2)(ii)(A)] **Section 2.2** ***Accurate Recording Process*** *Verify automatically the quality and accuracy of the storage media recording process.* [SEC 17a-4(f)(2)(ii)(B)] **Section 2.3 Serialize the Original and Duplicate Units of Storage Media** *Serialize the original and, if applicable, duplicate units of storage media, and time-date for the required period of retention the information placed on such electronic storage media.* [SEC 17a-4(f)(2)(ii)(C)] ***Section 2.4 Capacity to Download Indexes and Records*** *Have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable under this paragraphm as required by the Commission or the self-regulatory organizations of which the member, broker, or dealer is a member.* [SEC 17a-4(f)(2)(ii)(D)]
(ii) Systems that ensure the records entity is able to produce electronic regulatory records[6] 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 Azure Storage capabilities described in Section 2.5, including four options for duplicating the Blobs (records), meet the CFTC requirements (c)(2)(ii) to *ensure the availability of such regulatory records in the event of an emergency or other disru9.tion of the records entity's electronic record retention systems.* To satisfy this requirement for other essential data related to how and when the Blob (records) were created, formatted, or modified, the regulated entity must retain this data in a compliant manner.	***Section 2.5 Duplicate Copy of the Records Stored Separately*** *Store separately from the original, a duplicate copy of the record stored on any medium acceptable under §240.17a-4 for the time required.* [SEC 17a-4(f)(3)(iii)]

[6] 17 CFR § 1.31(a) includes indices *(Any data necessary to access, search, or display any such books and records)* in the definition of regulatory records.

CFTC 1.31(c)-(d) Requirement	Compliance Assessment Relative to CFTC 1.31(c)-(d)	SEC 17a-4(f) Requirements Listed in the Referenced Sections
(iii) The creation and maintenance of an *up-to-date inventory* that identifies and describes each system that maintains information necessary for accessing or producing electronic regulatory records.	The regulated entity is required to create and retain an *up-to-date inventory,* as required for compliance with 17 CFR § 1.31(c)(iii).	N/A
(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* ***12.a12.er*** *regulato11. records.* ***	It is Cohasset's opinion that Azure Storage has features that support the regulated entity's efforts to comply with requests for inspection or production of Blobs (records) and associated system metadata (i.e., index attributes). Specifically, it is Cohasset's opinion that Section 2.4, *Capacity to Download Indexes and Records,* describes use of Azure Storage to retrieve and download the Blobs (records} and the system metadata retained by Azure Storage. As noted in the *Additional Considerations* in Section 2.4.4, the regulated entity is obligated to produce the Blobs (records} and associated metadata, in the form and medium requested. If the regulator requests additional data related to how and when the Blobs (records) were created, formatted, or modified, the regulated entity willneed to provide this information from appropriate source systems	***Section 2.4 Capacity to Download Indexes and Records*** *Have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable under this paragraphm as required by the Commission or the self-regulatory organizations of which the member, broker, or dealer is a member.* [SEC 17a-4(f)(2)(ii)(D)]
(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*** *regulato11. records.* ***		

4 | Conclusions

Cohasset assessed the capabilities of Azure Storage, utilized with the *Immutable Storage for Azure Blobs* feature and the *Policy Lock* option, in comparison to the five requirements related to recording, storage and retention of record objects and associated metadata, as set forth in SEC Rule 17a-4(f) and its associated Interpretive Releases. Cohasset also correlated the principles-based requirements in CFTC Rule 1.31(c)-(d) to the assessed capabilities of Azure Storage.

Cohasset determined that Azure Storage, utilized with the *Immutable Storage for Azure Blobs* feature and the *Policy Lock* option, has the following capabilities which meet the regulatory requirements:

- Retains Blobs (records) in a non-erasable, non-rewriteable format, by applying integrated control codes at the Container level, to manage time-based[7] retention periods and legal holds. These retention controls prevent deleting, overwriting or changing a Blob (record) for the applied retention period or while subject to one or more legal holds. Additionally, Blobs (records) with a retention expiration date that has past remain protected from being overwritten or changed.
- Verifies the accuracy and quality of the recording process through checksums and Azure Storage validation processes, in addition to the inherent capabilities of advanced magnetic storage technology.
- Serializes each Blob (record) with an immutable, unique Object ID and storage date and time.
- Utilizes both replication and erasure coding when writing Blobs (records) to Azure Storage. If a Blob (record) is determined to be compromised, i.e., lost or damaged, an accurate replica is restored from a duplicate or regenerated from remaining valid erasure coded segments.
- Provides the capacity to (a) locate Blobs (records) and associated metadata (index) attributes, and (b) download the desired Blobs (records) and metadata (index) attributes so they may be transferred by the regulated entity in the format and media requested for production.

Accordingly, Cohasset concludes that Azure Storage capabilities, utilized with the *Immutable Storage for Azure Blobs* feature and the *Policy Lock* option to store and retain time-based Blobs (records), meet the five requirements of SEC Rule 17a-4(f). In addition, these capabilities meet the principles-based technology requirements of CFTC Rule 1.31(c)-(d).

[7] Time-based retention periods require the Blob (record) to be retained for a specified contiguous period of time, calculated from the date created/stored.

5 | Overview of Relevant Regulatory Requirements

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

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

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

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

- The Rule itself, as modified over time by the SEC. These modifications to the original Rule have not affected the requirements for electronic storage media, which are the basis of this assessment. However, certain Interpretive Releases have clarified the context and meaning of certain requirements and conditions of the Rule.
- SEC Interpretive Release No. 34-44238, *Commission Guidance to Broker-Dealers on the Use of Electronic Storage Media under the Electronic Signatures in Global and National Commerce Act of 2000 with Respect to Rule 77a-4(f),* dated May 1, 2001 (the "2001 Interpretive Release").
- SEC Interpretive Release No. 34-47806, *Electronic Storage of Broker-Dealer Records,* dated May 7, 2003 (the "2003 Interpretive Release").

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

> *(fJ The records required to be maintained and preserved pursuant to §§ 240.1la-3 and 240.7la-4 may be immediately produced or reproduced on "micrographic media" (as defined in this section) or by means of "electronic storage media" (as defined in this section) that meet the conditions set forth in this paragraph and be maintained and preserved for the required time in that form.*
>
> *(7) For purposes of this section:*
>
> *(ii) The term electronic storage media means any digital storage medium or system and, in the case of both paragraphs (f)(l)(i) and (f)(l)(ii) of this section, that meets the applicable conditions set forth in this paragraph {f).* [emphasis added]

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

> **SUMMARY:** *The Securities and Exchange Commission ("Commission") is amending its broker-dealer record preservation rule to allow broker-dealers to employ, under certain conditions, electronic storage media to maintain records required to be retained. The amendments reflect a recognition of technological developments that will provide economic as well as time-saving advantages for broker-dealers by expanding the scope of recordkeeping options while at the same time continuing to require broker-dealers to maintain records in a manner that preserves their integrity. The Commission is also issuing an interpretation of its record preservation rule relating to the treatment of electronically generated communications.*
>
> ***
>
> ***II. Description of Rule Amendments***
>
> ***A. Scope of Permissible Electronic***
>
> ***Storage Media***
>
> ****The Commission is adopting a rule today which, instead of specifying the type of storage technology that may be used, sets forth standards that the electronic storage media must satisfy to be considered an acceptable method of storage under Rule 1la-4. Specifically, because optical tape, CD-RO/VI, and certain other methods of electronic storage are available in WORM and can provide the same safeguards against data manipulation and erasure that optical disk provides, the final rule clarifies that broker-dealers may employ any electronic storage media that meets the conditions set forth in the final rule.*[8] [emphasis added]

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

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

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

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

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

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

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

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

> *Moreover, there may be circumstances (such as receipt of a subpoena) where a broker-dealer is required to maintain records beyond the retention periods specified in Rule 1la-4 or other applicable Commission rules. Accordingly, a broker-dealer must take appropriate steps to ensure that records are not deleted during periods when the regulatory retention period has lapsed but other legal requirements mandate that the records continue to be maintained, and the broker-dealer's storage system must allow records to be retained beyond the retentions periods specified in Commission rules.* [emphasis added]

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

See Section 2, *Assessment of Compliance with SEC Rule 7la-4({),* for a list of each SEC electronic records storage requirement and a description of the capabilities of Azure Storage related to each requirement.

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

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

> *(c)All books and records required to be made pursuant to the FINRA rules shall be preserved in a format and media that complies with SEA [Securities Exchange Act] Rule 1la-4.*

5.3 Overview of CFTC Rule 1.31 Electronic Regulatory Records Requirements

Effective August 28, 2017, the Commodity Futures Trading Commission (CFTC) amended 17 CFR § 1.31 ("CFTC Rule") to define principles-based requirements for organizations electing to retain electronic regulatory records. The CFTC requirements for electronic regulatory records evolved through amendments to Rule 1.31. The most substantive changes included:

- The June 28, 1999, amendment first implemented the technical provisions regarding the use of electronic storage media for required books and records.
- The November 2, 2012, amendment clarified the retention period for certain oral communications.
- The August 28, 2017, amendments modernize and make technology-neutral the form and manner in which regulatory records, including electronic regulatory records, must be retained and produced.

To address the transition to electronic regulatory records, the CFTC amended and modernized its recordkeeping regulation to adopt principles-based standards that are less prescriptive. This resulted in rephrasing and modernizing the requirements previously defined in 1999, as explained in the August 28, 2017, Federal Register in *Ill. Final Rules, D. Regulation 7.37(c): Form and Manner of Retention:*

> *Consistent with the Commission's emphasis on a less-prescriptive, principles-based approach, proposed§ 1.31(d)(1) would rephrase the existing requirements in the form of a general standard for each records entity to retain all regulatory records in a form and manner necessary to ensure the records' and recordkeeping systems' authenticity and reliability. The Commission proposed to adopt§ 1.31(d)(2) to set forth additional controls for records entities retaining electronic regulatory records. The Commission emphasized in the Proposal that the proposed regulatory text does not create new requirements, but rather updates the existing requirements so that they are set out in a way that appropriately reflects technological advancements and changes to recordkeeping methods since the prior amendments of§ 1.31 in 1999.* [emphasis added]

The definitions established in 17 CFR § 1.31(a) are paramount to applying the CFTC requirements.

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

These definitions establish that recordkeeping obligations apply to (a) all *records entities,* without exception, and (b) all *regulatory records.* Further, for *electronic regulatory records,* paragraphs (i) and (ii) establishes an expanded definition of an electronic regulatory record to include information describing data necessary to access, search and display record objects, as well as information describing how and when such books and records were created, formatted, or modified.

The retention time periods for regulated records includes both time-based[9] and event-time-based[10] retention periods. Specifically, 17 CFR § 1.31 (b)(1)-(b)(3) states:

> ***Duration of retention.*** *Unless specified elsewhere in the Act or Commission regulations in this chapter:*
>
> *(1) A records entity shall keep regulatory records of any swap or related cash or forward transaction (as defined in § 23.200(i) of this chapter), other than regulatory records required by§ 23.202(0)(1) and (b)(1)-(3) of this chapter, from the date the regulatory record was created until the termination, maturity, expiration, transfer, assignment, or novation date of the transaction and for a period of not less than five years after such date.*
>
> *(2) A records entity that is required to retain oral communications, shall keep regulatory records of oral communications for a period of not less than one year from the date of such communication.*
>
> *(3) A records entity shall keep each regulatory record other than the records described in paragraphs (b)(1) or (b)(2) of this section for a period of not less than five years from the date on which the record was created.* [emphasis added]

For a list of the CFTC principles-based requirements and a summary assessment of the capabilities of Azure Storage related to each requirement, see Section 3, *Summary Assessment of Compliance with CFTC Rule 7.37(c)-(d).*

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

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

About Cohasset Associates, Inc.

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

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

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

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

For domestic and international clients, Cohasset:

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

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

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

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