Cohasset Associates

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

Microsoft Security & Compliance Center with Exchange Online

Abstract

Exchange Online is a Microsoft Office 365 cloud-based service for email and mailbox items (often referred to as Outlook) and communications archived from Skype for Business Online and Microsoft Teams. Exchange Online, in conjunction with the Security and Compliance Center, was designed to meet securities industry requirements for preserving electronic records in a non-rewriteable and non-erasable format, by protecting each electronic record from being modified, overwritten or deleted until it has been stored for the applied retention period and legal holds.

This report documents the assessment conducted by Cohasset Associates, Inc. ("Cohasset") of the capabilities of Exchange Online, together with certain features of the Security and Compliance Center, relative to the electronic records storage, retrieval and management requirements of the:

- 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.

When compliance features are properly configured, carefully applied and managed, as described in this Assessment Report, it is Cohasset's opinion that the assessed Office 365 services meet the non-rewriteable, non-erasable (WORM) requirement by applying *Compliance Retention Policies* (with *Preservation Lock*), together with *eDiscovery Holds,* to records stored in Exchange Online, including data archived by Skype for Business Online and Microsoft Teams. Further, the assessed Office 365 services (together with planned enhancements to the audit system, see sections 2.12 and 2.13) meet or support the regulated entities' efforts to achieve compliance with the other requirements of the Rule.

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

1 | 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, 2017, 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.

Microsoft has enhanced certain Exchange Online services to support compliance with these stringent electronic records storage, retrieval and management requirements. To evaluate its compliance with SEC Rule 17a-4(f) and CFTC Rule 1.31(c)-(d), Microsoft engaged Cohasset to complete an independent and objective assessment of the capabilities of Exchange Online services, when compliance features are properly configured and used, relative to these requirements.

This Introduction briefly summarizes the regulatory environment, explains the purpose and approach for Cohasset's assessment, and provides an Executive Summary of the assessment scope and findings.

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 17a–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.

1.1.2 FINRA Rule 4511(c) Requirements

Financial Industry Regulatory Authority (FINRA) Rule 4511(c) states: *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 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."

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. Where feasible, Cohasset used the term *record* to recognize that the data or object is a regulated record.

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 electronic records 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 the assessed Office 365 services, 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 the Security and Compliance Center, together with Exchange Online, when compliance features are properly configured and used, in comparison to the 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 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.

Cohasset was engaged to:

- Perform an assessment of the capabilities of the Security and Compliance Center, together with Exchange Online, when compliance features are properly configured and used, in comparison to the seventeen electronic storage requirements, 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 the Office 365 services; see Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d);* and
- Prepare this Assessment Report, enumerating the results of its assessment.

In addition to applying the information in this Assessment Report, regulated entities must ensure that the combination of its policies, procedures and regulatory submissions, in conjunction with the capabilities of implemented electronic recordkeeping solutions, meet all applicable requirements of SEC Rule 17a-4(f) and CFTC Rule 1.31.

This assessment represents the professional opinion of Cohasset and should not be construed as either an endorsement or a rejection by Cohasset of Microsoft Exchange Online, Office 365 or other Microsoft products or services. The information utilized by Cohasset to conduct this assessment consisted of: (a) oral discussions, (b) technical articles, and (c) 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 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 the report.

Exchange Online is a cloud-based Office 365 service that retains and manages mailbox items and certain archived items from Skype for Business Online and Microsoft Teams. The Security and Compliance Center, also an Office 365 service, provides key compliance features such as *Compliance Retention Policies*[3] and *eDiscovery Holds*.

This Assessment Report focuses on these compliance features how they are executed within Exchange Online.

- To enable compliance with the non-rewriteable, non-erasable (WORM) requirement, a *Compliance Retention Policy,* with *Preservation Lock,* must be applied to regulated records, in the following Locations.
  - User, shared, resource and group mailboxes in Exchange Online[4]
  - Exchange Public Folders
  - Skype for Business Online
  - Teams Channel Messages
  - Teams Chats

  See the beginning of Section 2, *Assessment of Compliance with SEC Rule 17a-4(f),* for details on content that is included and excluded for compliance with the Rule.
- The retention periods set for the policies must meet or exceed the retention requirements established by regulators and self-regulatory organizations, e.g., FINRA.
  - Only time-based[5] retention periods are supported by *Compliance Retention Policies*. Event-based[6] retention periods are supported by *Retention Labels*, which may be applied to mailbox items in addition to *Compliance Retention Policies*.
  - Once archiving and the *Compliance Retention Policies*, with *Preservation Lock*, are configured and applied, records are automatically protected for compliance. These *locked* policies are integrated control codes, which

[3] For compliance with SEC Rule 17a-4(f), the Preservation Lock feature must be applied to the Compliance Retention Policy.

[4] Exchange Online is the backend email solution that retains mailbox items, which are accessed, by users, via the Outlook interfaces.

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

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

extend protections to the storage solution, by *preventing* (a) shortening the retention period of the policy, (b) removing the policy from a record, and (c) overwriting, changing and deleting the record by users and by lifecycle processes, until after expiration of the associated retention policy(ies). Individual users are *not* required to take additional steps.

- *eDiscovery Holds* must be applied to records required for litigation, subpoena and other similar circumstances.
- These policies ensure that the records and the associated properties and metadata attributes (index information) are immutable (unchangeable) and cannot be modified, overwritten or deleted until the applied retention periods are expired and any *eDiscovery Holds* are cleared. Thereafter, the records remain immutable (unchangeable and non-overwritable), though eligible records may be deleted.
- When a record in the mailbox is deleted (by a user or by a policy), *but ongoing retention is required by another Compliance Retention Policy or eDiscovery Hold*, the record is retained in a background archive[7] in Exchange Online and until all applied retention periods expire (the longest retention period wins) and any *eDiscovery Holds* are cleared.
- When a *Compliance Retention Policy* applies to mailbox items or archived records (from Skype for Business or Microsoft Teams) in a user or group mailbox, if the O365 account is deleted, the mailbox becomes *inactive*, rather than being deleted. An *inactive* mailbox will be retained for the duration of the *Compliance Retention Policies* that were applied before it became inactive. New *Compliance Retention Policies* cannot be applied to an *inactive* mailbox.
  - An *inactive* user or group mailbox may be *restored*[8], to provide access to the contents of the *inactive* mailbox, including archived Skype for Business, Teams Channel Messages or Teams Chats.
  - The regulated entity must **not** *recover*[9] an *inactive* mailbox that contains required books and records, because the policies will no longer apply after the mailbox is recovered.
- Office 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 attributes (index information), are replicated across at least two, and up to four, data centers.
- The creation (storage) date and time, unique identifier and version identifier serialize each record. These attributes are system-generated and cannot be edited by users or administrators.
- 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.
- 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.

---

7 The background archive for Exchange Online is the Recoverable Items Folder (RIF).

8 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.

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

- Records identified in a search may be reviewed and downloaded, together with key properties and metadata attributes (index information).
- 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 Exchange Online or Office 365 license agreement.
- Human-readable renditions of the stored records are generated using the source application or a viewer. Downloads are in standard formats, such as Personal Storage Table (.pst) files.
  - Teams Channel Messages and Teams Chats are stored as conversation segments, which must be manually assembled into a conversation chain. (Enhancements to store and retrieve threaded Teams Channel Messages and Teams Chats are planned for release in approximately July 2019.)
  - Emojis, giffies (GIFs), memes and stickers are stored as weblinks, which may change over time.
  - Reactions (e.g., likes/thumbs up) are ***not*** captured for compliance; therefore, reactions cannot be reproduced with the Teams Channel Message and Teams Chat where the reaction was applied. (Enhancements to store and retrieve reactions, together with Teams Channel Messages and Teams Chats, are planned for release in approximately July 2019.)
  - Similarly, reactions applied to mailbox items are ***not*** captured for compliance and, therefore, cannot be reproduced with the mailbox item where the reaction was applied.
- When downloading from Exchange Online, message content, properties and metadata attributes are downloaded, by default. In addition, authorized users may *Enable Full Logging*, which includes a complete list of each item found.
- Records include audit information, e.g., date/time, sender, recipients. In addition, mailbox-level auditing is available for user, shared and resource mailboxes. (Enhancements to Exchange auditing for Group Mailboxes are planned for release in approximately July 2019.) When mailbox auditing is properly configured and in combination with metadata for the mailbox items (e.g., date sent, sender and recipients), audit system data related to inputting and changing mailbox items are captured.
  - To preserve user, shared and resource mailbox-level audit data for the same time period as the record, the regulated entity must export and store audit log entries in a separate system for the required retention period.

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

This section presents Cohasset's evaluation of the capabilities of Exchange Online services, when compliance features are properly configured and used, for compliance with the seventeen electronic records requirements, which pertain to the recording, storage, retrieval, management and retention of electronic records, as stipulated in SEC Rule 17a-4(f).

Assessment Scope

This assessment pertains to certain electronic records stored and managed by Exchange Online, which is a cloud-based service for mailbox items and certain archived items from Skype for Business Online and Microsoft Teams. Additionally, the Security and Compliance Center provides key compliance features such as C*ompliance Retention Policies* and *eDiscovery Holds*.

To enable compliance with the SEC Rule 17a-4(f) requirement for a non-rewriteable, non-erasable (WORM) record format, a *Compliance Retention Policy*, with *Preservation Lock,* must be applied to regulated records. The following table describes the content that is *included in* and *excluded from* each Location for this Assessment Report.

Location	Included in the Assessment	***Excluded*** **from the Assessment**
• Exchange Online mailboxes (often referred to as Outlook)	• User, shared, resource and group mailboxes	• Site mailboxes. • Members of distribution lists, when more than 10,000 members or more than 25 nested levels. • Reactions (e.g., likes/thumbs up) applied to mailbox items, using Outlook Web Application (OWA). Options to disable this feature may be available.
• Exchange Public Folders	• Exchange Public Folders	• No items are excluded.
• Skype for Business Online[10]	• Peer-to-peer instant messaging • Web conferencing transcripts	• 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 Online collaboration elements *not* archived into Microsoft Exchange Online.

[10] Skype for Business content that may be stored in the Conversation History File in Exchange, is in addition to the compliance copy archived in Exchange Online; therefore, the Conversation History File is *not* relevant to this assessment.

Location	Included in the Assessment	***Excluded*** **from the Assessment**
• Teams Channel Messages	• Teams Channel Messages archived in hidden folders in Exchange Online	• Teams audio and video recordings. • Reactions (e.g., likes/thumbs up) in Teams Channel Messages and Teams Chats. (NOTE: Enhancements to store and retrieve reactions together with Teams Channel Messages and Teams Chats are planned for release in approximately July 2019.) • Note: For emojis, giffies (GIFs), memes and stickers, *only* weblinks are captured; and, these may change over time.
• Teams Chats[11]	• Non-guest Teams Chats archived in hidden folders in Exchange Online	• Teams Chats exclusively among guests[12]. • See above for Teams Channel Messages.

Assessment Organization

For each of the *seventeen* 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 capabilities of relevant Office 365 services
- ***Capabilities of Assessed Office 365 Services*** – Description of capabilities of the Office 365 services relevant to the specific requirement of the SEC Rule 17a-4(f)
- ***Additional Considerations*** – Additional considerations related to meeting the specific requirement

The following subsections document Cohasset's assessment of the capabilities of the Security and Compliance Center, in conjunction with Exchange Online services, when compliance features are properly configured and used, 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)]

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-erasable and non-rewriteable recording environment provided: (a) the storage solution delivers the prescribed functionality

[11] Microsoft Teams Channel Messages and Teams Chats stored in the Chat Service are in addition to the compliance copy archived in Exchange Online; therefore, the Chat Service is *not* relevant to this assessment.

[12] These Chats are archived into Exchange Online for eDiscovery. However, a *Compliance Retention Policy* cannot be applied, as of the date of this report.

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

When configured and managed, as described in Section 2.1.3 and 2.1.4, it is Cohasset's opinion that the assessed capabilities of the Security and Compliance Center, together with Exchange Online, meet the requirements of the Rule for (a) managing electronic records as non-rewritable and non-erasable (WORM) for the assigned retention period and (b) preserving electronic records for legal holds, as required. Specifically, properly configured and applied *Compliance Retention Policies*, with *Preservation Lock,* protect records in the storage solution through integrated control codes that *prevent* (a) shortening the retention period of the policy, (b) removing the policy from a record, and (c) overwriting, changing and/or deleting the record by users and by lifecycle processes, until after the expiration of associated retention policy(ies).

2.1.3 Capabilities of Assessed Office 365 Services

In this subsection, Cohasset presents the assessed capabilities of Exchange Online services that directly pertain to the requirement for preserving electronic records as non-rewritable and non-erasable, for the required retention period and any associated legal holds.

2.1.3.1 General Overview

- The Security and Compliance Center is a data protection and governance portal, which provides centralized access to wizards, used to define *Compliance Retention Policies*[13] and *eDiscovery Cases* (legal holds). These *features*, are designed for: (1) retaining records, (2) preserving records for legal holds, such as subpoena and litigation, (3) protecting records in a *non-rewriteable, non-erasable format [for the required retention period and*

[13] For compliance with SEC Rule 17a-4(f), the Preservation Lock feature must be applied to the Compliance Retention Policy.

applicable legal holds] in compliance with SEC Rule 17a-4(f)(2)(ii)(A), and (4) optionally, automating the deletion of eligible records.

  - For compliance with the non-rewriteable, non-erasable format requirement of the Rule, this assessment report describes how these Security and Compliance Center features must be used.

- *Retention Labels*, which are also configured using the Security and Compliance Center, are *excluded* from this assessment, because they cannot be applied to the mailbox or to system folders (e.g., the Inbox, Sent Items folder, calendar, etc.) and cannot be applied to records archived by Skype for Business Online or Microsoft Teams.
- *Legacy* policies (e.g., Default Policy Tags, Retention Policy Tags, Personal Policy Tags, etc.), are also *excluded* from this assessment.

2.1.3.2 Principle of Immutability

- When a *Compliance Retention Policy* or *eDiscovery Hold* is applied to a record in Exchange Online:
  - The record content is immutable, and
  - Key properties and metadata attributes, such as creation (storage) date and time and the universal identifier are immutable.
- These immutability protections apply until the record is deleted. Thus, even if the retention period expires for a specific record, and it is not subject to a legal hold, it will remain immutable.

2.1.3.3 Compliance Retention Policies with Preservation Lock

For compliance with the non-rewritable, non-erasable requirement of SEC Rule 17a-4(f), *Compliance Retention Policy(ies)*, with *Preservation Lock*, must be configured and applied to each regulated record stored or archived into Exchange Online. A properly configured and applied *Compliance Retention Policy*, with *Preservation Lock,* protects records in the storage solution through integrated control codes. A *locked* policy is required for compliance with SEC Rule 17a-4(f), because its integrated control codes prevent both: (a) shortening the retention period of the policy and (b) removing the policy from a record. In addition, integrated control codes prevent overwriting, changing and deleting the record by users and by lifecycle processes, until after expiration of the associated retention policy(ies).

- *Compliance Retention Policy(ies)* must be configured with an appropriate time-based retention period; optionally, a delete action may be set. (Event-based retention periods are supported by *Retention Labels*, which may be applied to mailbox items in addition to *Compliance Retention Policies.)*
- The *Preservation Lock* feature must be applied to the *Compliance Retention Policy* for SEC 17a-4(f) compliance. This enables the following controls:
  - The *Compliance Retention Policy* cannot be deleted.
  - The retention period cannot be shortened; its duration can only be lengthened.
  - Locations cannot be removed from the policy; only new Locations can be added. Further, the scope can be expanded, but cannot be decreased. For example, Exchange Online mailboxes can be added or query terms can be expanded, but neither can be subsequently removed or more narrowly defined.

- As described in the *Assessment Scope* (beginning of Section 2), for compliance with Rule 17a-4(f), a *Compliance Retention Policy*, with *Preservation Lock*, must be applied to regulated records in:
  - **User, shared, resource and group Exchange mailboxes**:
    - Each active mailbox is automatically processed *at least* every 7 days to apply retain and delete actions. Optionally, the client administrator may manually initiate the process, at any time.
  - **Exchange Public Folders**:
    - Only the retain actions apply to records in Public Folders; delete actions do ***not*** apply.
    - When set, the *Compliance Retention Policy* applies to all items stored in Public Folders.
  - **Skype for Business Online** records archived into hidden folders in Exchange Online:
    - When archiving is configured and a user is specified in a *Compliance Retention Policy*, archiving is triggered within the Skype environment to capture certain Skype content within Exchange.
    - The Conversation History is separate and does *not* retain the regulated record; therefore, Conversation History is out-of-scope for this assessment.
  - **Teams Channel Messages** archived into hidden folders in Exchange Online:
    - The Chat Service is separate and retains a copy of current Teams Channel Messages. These copies are separate from the *immutable archived copy*, which is retained as the regulated record. Therefore, the Chat Service is out-of-scope for this assessment.
  - **Teams Chats** archived into hidden folders in Exchange Online:
    - Applies to Teams Chats that include at least one authenticated user; a *Compliance Retention Policy* cannot be applied to Teams Chats *exclusively* among guests.
    - The Chat Service is separate and retains a copy of current Teams Chats. These copies are separate from the *immutable archived copy*, which is retained as the regulated record. Therefore, the Chat Service is out-of-scope for this assessment.
- When a *Compliance Retention Policy* applies to a record:
  - The record is immutable for its lifespan, including after the retention period expires and any *eDiscovery Holds* are cleared.
  - Versions are automatically saved. For example, if the Subject of an email is updated, a copy of the email is saved in the background archive, before the change is applied.
  - When a record is deleted (by a user or by another policy) from the users' view of the mailbox, but ongoing retention is required by a *Compliance Retention Policy* or *eDiscovery Hold*, the record is copied to the associated background archive, and retained until the *longest* retention period expires and all *eDiscovery Holds* are cleared. In other words, the *longest* retention period wins in the background archive.
    - Deleted mailbox items that are eligible for deletion (no policy requires retention) are kept in the background archive for a minimum of 14 days, which may be extended up to 30 days. Additionally, calendar items deleted after they are eligible are retained for 120 days.

    - If the query of applied Compliance Retention Policies becomes lengthy or complex, actions to delete items are not processed.
  - Further, when the *Preservation Lock* feature is applied to the *Compliance Retention Policy* it cannot be removed from the Location, for any reason; therefore, it cannot be removed from the record.
- If multiple *Compliance Retention Policies* apply to a record:
  - It is removed from the user's view, after expiration of the *shortest* retention period of the applied *Compliance Retention Policies*.
  - It is retained in the background archive, to satisfy the *longest* retention period of the applied *Compliance Retention Policies*.
- When a *Compliance Retention Policy* applies to mailbox items or archived records (from Skype for Business, Teams Channel Messages or Teams Chats) in a user or group mailbox, if the O365 account is deleted, the mailbox becomes *inactive*, rather than being deleted. An *inactive* mailbox will be retained for the duration of the *Compliance Retention Policies* applied before it became inactive. New *Compliance Retention Policies* cannot be applied to an *inactive* mailbox.
  - An *inactive* user or group mailbox may be *restored*, to provide access to the contents of the *inactive* mailbox, including archived Skype for Business, Teams Channel Messages or Teams Chats.
    - The *inactive* mailbox is preserved and remains an *inactive* mailbox.
    - A *copy* of the contents of the *inactive* mailbox is incorporated into the other existing mailbox.
  - The regulated entity must **not** *recover* an *inactive* mailbox that contains required books and records, because the policies will no longer apply after the mailbox is recovered.
- The *HoldCleanup* parameter may be used to remove duplicate versions of mailbox items from the background archive. An administrator may run this command in scenarios where the background 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.

2.1.3.4 Legal Holds

- An *eDiscovery Hold, created and accessed from the Security and Compliance Center* preserves records subject to a legal hold. *eDiscovery Holds* require the creation of a legal case. Advanced search criteria may then be entered to locate relevant content in Exchange Online. Once identified, the records will be associated with the selected case and preserved indefinitely by the *eDiscovery Hold* feature. Results can be exported for further analysis.
- eDiscovery Managers can perform searches and place holds on records in Exchange online, including: (a) user, shared, resource and group mailboxes in Exchange, (b) Exchange Public Folders, (c) Skype for Business Online archived into hidden folders in Exchange, and (d) Teams Channel Messages and Teams Chats (including Teams Chats *exclusively* among guests) archived into hidden folders in Exchange.
- The limits for *eDiscovery Holds* are:
  - Maximum of 10,000 case holds for an organization

- Maximum of 1,000 mailboxes in a single case hold

- When the legal hold is resolved, the associated *eDiscovery Hold* should be cleared, at which time, preservation control will be returned to other applied policies.

2.1.3.5 Clock Management

- Exchange Online 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 Exchange Online servers.

2.1.3.6 Security

Accordingly, the following security features apply to Exchange Online.

- 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 Office 365, including physical data center security, network security, access security, application security, and data security. Office 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 Office 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 Office 365 services is secured using TLS/SSL communications security protocol.

2.1.4 Additional Considerations

For the Locations in Exchange Online 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, resource or group mailboxes in Exchange Online; (b) Exchange Public Folders; (c) Skype for Business, Teams Channel Messages and Teams Chats, archived into hidden folders in Exchange Online.
- Applying a *Compliance Retention Policy*, with *Preservation Lock*, to 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.
- Utilizing other recordkeeping solutions for regulated records that are *excluded* from this assessment, or are *not* protected by a *Compliance Retention Policy*, with *Preservation Lock*, as explained in the *Assessment Scope*.
- Enabling the *archiving* feature in Skype for Business for each user, with regulated records.

- Configuring Skype for Business to require guests to wait in the Meeting Lobby until the meeting organizer (which must be an authenticated user) opens the meeting and admits the participants, since at least one member of the interaction must be logged in as an authenticated user for the Skype for Business content to be archived.

- Monitoring logs and quotas to ensure contractual storage limits are not exceeded and that In-Place Archive mailboxes are established, as required for expanded storage.
- 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 Office 365 services.
- Establishing procedures to prohibit administrators from taking actions that impair compliance with the Rule and monitoring to assure compliance. For example, procedurally prohibit assignment of the *Mailbox Import Export* role and disallow the *recover* process for inactive mailboxes.
- 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 cleared or until the records have been transferred to another compliant solution.

2.2 Accurate Recording Process

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

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

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

2.2.2 Compliance Assessment

It is Cohasset's opinion that the assessed capabilities of Exchange Online, in conjunction with the inherent capabilities of advanced storage technology, meet this requirement of the Rule.

2.2.3 Capabilities of Assessed Office 365 Services

Exchange Online utilizes 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 calculated and stored to enable post-recording integrity verification.
- 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 one of the valid replicas.

2.2.4 Additional Considerations

There are no additional considerations related to this requirement.

2.3 Serialize the Original and Duplicate Units of Storage Media

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

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

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

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

2.3.2 Compliance Assessment

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

2.3.3 Capabilities of Assessed Office 365 Services

- Office 365 services systematically apply and retain system-generated creation (storage) date and time and a unique Item identifier, along with Change Key (version) for each record. This serializing information is an integral part of the metadata for each duplicate/replica made for data resiliency.
  - For mailbox items, the system-generated date and times include: (a) creation date and time for items created in Exchange and (b) received date and time for items received by Exchange, including sent items and imported or ingested items (e.g., email messages from third party sources).

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)]

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

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

2.4.2 Compliance Assessment

It is Cohasset's opinion that the combination of capabilities of the Office 365 Security and Compliance Center, together with Exchange Online, meet this SEC requirement to readily download indexes and regulated records, by: (a) maintaining hardware and software capacity and high data availability and (b) providing Internet-based search capabilities to authorized users to (i) search, (ii) view search metrics and results, and (iii) export search results, which may be copied to compliant media. These records, together with properties and metadata attributes (index information), can then be transferred, by the regulated entity, in the format and media requested for production.

2.4.3 Capabilities of Assessed Office 365 Services

Exchange Online is cloud-based and designed for high availability and site resilience. As a commitment to running a highly available service, Microsoft has a Service Level Agreement of 99.9% that is financially-backed. Accordingly, Internet connection services are the primary equipment capacity needed to download indexes and records.

eDiscovery Managers and other authorized users may initiate searches and download the indices and records using the Security and Compliance Center features, with or without setting up an eDiscovery case.

Exchange Online Content Search and Export Features

- Authorized users may perform content searches to find and select items stored in Exchange Online, including the Primary and In-Place Archive mailboxes and associated background archives. Search criteria includes message recipients, senders, subject, date sent or received, etc.
- The results 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 attributes (index information) are downloaded.
  - Options when copying messages to a discovery mailbox include:
    - **Enable de-duplication**, which eliminates duplications and stores only one copy of an item.
    - **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 PST file, which includes the items and index metadata, may be copied to a storage medium that complies with the requirements of the Rule.

Additional Search Capabilities

- Full-text searches query text-based records.
- 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.

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.

Additional Export Capabilities

- Search results may be previewed, after executing a search in the Security and Compliance Center.
- When downloading Exchange Online messages, properties and metadata attributes are downloaded, by default. In addition, authorized users may *Enable Full Logging*, which includes a complete list of each item found. Even if the messages are de-duplicated, this log contains the specifics about each instance of the message, e.g., one user's mailbox had it in the Inbox and flagged as important, but another user's mailbox had it moved it to the Deleted Items folder without reading it.
- Several reports document the process, including, but not limited to, an Export Summary, Manifest of each exported item, Results log for each exported item, and a Trace Log containing information about the export process.

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 sent a message on behalf of another mailbox owner, the message will be in the Sent items of the delegate.
- Delays of up to 24 hours may be experienced for the index and audit logs to be updated and findable in searches.
- The regulated entity is responsible for (a) maintaining its account in good standing, (b) authorizing appropriate user access, (c) maintaining hardware and software to access Office 365 services, (d) maintaining its encryption keys that have been used in addition to the Customer Key service, (e) transferring the records and associated index data to a compliant storage medium, as required, and (f) assuring that the regulator, self-regulatory organization or designated examining authority receive downloads of the records, properties and metadata attributes (index information), in the requested format and medium.

2.5 Readable Projection or Production of Images for Examination

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

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

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 easily readable images.

2.5.2 Compliance Assessment

Cohasset believes Exchange Online meets this requirement by allowing authorized users to search, select, view and print electronic records using an Internet browser or other local tools to render a human-readable image.

2.5.3 Capabilities of Assessed Office 365 Services

- Exchange Online 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.
  - Installed applications on the users' computers, laptops and other compatible devices, as part of the Office 365 license agreement.
- More restrictive access may be granted to some devices, such as smartphones.
- Additionally, authorized users may conduct content searches, using the Security and Compliance Center. See Section 2.4.3.
- 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 email 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 to render a view of the attachment.
- Additionally, these decrypted electronic records and associated attachments may be printed.

2.5.4 Additional Considerations

- Teams Channel Messages and Teams Chats are stored and displayed in Messaging Application Programming Interface (MAPI) format, which does not display the original look-and-feel of the communication chain:
  - Individual message segments can be retrieved from Exchange Online and then analyzed and organized to assemble the conversation chain. (Enhancements to store and retrieve threaded Teams Channel Messages and Teams Chats are planned for release in approximately July 2019.)
  - 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.
  - Reactions (e.g., likes/thumbs up) are *not* captured for compliance; therefore, they cannot be reproduced together with the Teams Channel Message and Teams Chat where the reaction was applied. (Enhancements to store and retrieve reactions together with Teams Channel Messages and Teams Chats are planned for release in approximately July 2019.)
- Similarly, reactions (e.g., likes/thumbs up) applied to mailbox items are *not* captured for compliance; therefore, they cannot be reproduced together with the mailbox items where the reaction was applied.
- Optionally, emojis, giffies (GIFs), memes and stickers may be disabled on a *per site* basis.
- See also Section 2.4.4, *Additional Considerations*, for the *Capacity to Download Indexes and Records* section.

2.6 Reproduction of Images Provided to Regulators

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

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

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

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.*

2.6.2 Compliance Assessment

It is Cohasset's opinion that the combination of capabilities of the Security and Compliance Center, together with Exchange Online, support meeting this requirement, by providing authorized users the capability to search, select, reproduce and download copies of the records.

2.6.3 Capabilities of Assessed Office 365 Services

- Authorized users may search and export content, using Security and 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.

2.6.4 Additional Considerations

- The reproductions of Teams Channel Messages and Teams Chats do not display the (a) look-and-feel of the communication chain or (b) associated reactions (e.g., likes/thumbs up). (Enhancements to store and retrieve reactions together with Teams Channel Messages and Teams Chats are planned for release in approximately July 2019.)
- The reproductions of email messages do not display associated reactions (e.g., likes/thumbs up) applied to mailbox items, using Outlook Web Application (OWA).
- Stored weblinks are provided, in lieu of emojis, giffies (GIFs), memes and stickers.
- See also Section 2.4.4, *Additional Considerations*, for 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)]

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.

2.7.2 Compliance Assessment

It is Cohasset's opinion that the assessed capabilities of Exchange Online meet this requirement of the Rule, since more than one replica of all records (including content and metadata) is stored.

2.7.3 Capabilities of Assessed Office 365 Services

- Each 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 replica 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.
- Exchange Online 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 background archive. Deleted calendar items are stored for 120 days and other mailbox items are retained for 14 to 30 days, depending on the configuration.

2.7.4 Additional Considerations

There are no additional considerations related to this requirement.

2.8 Organization and Accuracy of Indexes

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

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

> **SEC 17a-4(f)(3)(iv):** Organize and index accurately all information maintained on both original and any duplicate storage media.

2.8.2 Compliance Assessment

Cohasset believes that this requirement is met by Exchange Online, because properties and metadata attributes (index information), for records included in the *Assessment Scope*, are stored for the same period of time as the corresponding electronic record.

2.8.3 Capabilities of Assessed Office 365 Services

- Authorized users may organize records in a folder hierarchy in Exchange Online mailboxes and Public Folders. Additionally, Teams Channel Messages and Teams Chats among non-guests are organized chronologically in hidden folders in Exchange Online.
- Each record includes properties and metadata attributes that serve as an index and permit authorized users to sort and organize the records.
- The accuracy of the properties and metadata attributes (index information) is supported by utilizing system-generated attributes and from searching controlled data sources, such as the To, CC, BCC and From names for an email message and full-text search of immutable content.

2.8.4 Additional Considerations

There are no other considerations related to this requirement.

2.9 Availability of Indexes for Examination

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

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.

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

2.9.2 Compliance Assessment

It is Cohasset's opinion that the combination of capabilities of the Security and Compliance Center, together with Exchange Online, meet this requirement of the Rule, by providing authorized users capabilities to search, retrieve and export properties and metadata attributes (index information).

2.9.3 Capabilities of Assessed Office 365 Services

- Authorized users may run content searches (see Section 2.4.3) to find records; and then, review, access and download properties and metadata attributes (index information) for the selected records.
- When copying Exchange Online messages to a discovery mailbox, by default properties and metadata attributes are downloaded.

2.9.4 Additional Considerations

- See Section 2.4.4, *Additional Considerations*, for 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)]

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

> **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 each index.

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

2.10.2 Compliance Assessment

It is Cohasset's opinion that the capabilities of Exchange Online meet this requirement of the Rule, since more than one replica of the properties and metadata attributes (index information) are stored.

2.10.3 Capabilities of Assessed Office 365 Services

- At the time of recording in Exchange Online, one or more duplicate copies of each item *and its associated properties and metadata attributes (index information)* are automatically created and stored, to provide high availability and site resilience.
- Index data is stored together with the mailbox.
- Exchange Online 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.

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)(C)]

This requirement ensures that both the original and duplicate index is preserved for the same period of time as the indexed record itself (and the duplicate of the record). Accordingly, the records cannot become inaccessible as a result of the index not being retained as long as the associated records.

> **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 asserts that Exchange Online meets this SEC requirement to preserve properties and metadata attributes (index information) for the same retention period as the corresponding regulated records.

2.11.3 Capabilities of Assessed Office 365 Services

- At the time of recording in Exchange Online, the properties and metadata attributes, which serve as *index* information, are simultaneously created and stored, to provide high availability and site resilience.
- The properties and metadata attributes (index information) 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

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

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

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

2.12.2 Compliance Assessment

It is Cohasset's opinion that a combination of the record attributes, e.g., date/time, sender, recipients, etc., and the audit system features described in Section 2.12.3, when properly configured and utilized to capture and maintain the audit results, *support* efforts to meet this requirement of the Rule to create an audit trail of inputting and changing regulated records. (Audit enhancements for Group Mailboxes, planned for release in approximately July 2019, will further support these audit requirements.)

2.12.3 Capabilities of Assessed Office 365 Services

- The Office 365 Management APIs provide a single extensibility platform for Office 365 auditing, as well as service communications, security, compliance and reporting. These audit results are retained, by default, for a minimum of 90 days.

Security and Compliance Center Audit System

- When audit logging is enabled, authorized users may search available audit results, using the Security and Compliance Center or Office 365 Management APIs.
  - Actions logged include, but are not limited to:
    - Create, modify, or delete a *Compliance Retention Policy*.
    - Perform eDiscovery-related activities, such as (a) creating and managing eDiscovery cases, (b) creating, starting, and editing content searches, (c) previewing, exporting, and deleting search results, (d) configuring permissions filtering for content search, and (e) managing the eDiscovery Manager role.
  - For each action taken, the audit details include the following:

- Action taken
- User taking the action.
- Date and time of the action.
- Identifier (e.g., *Compliance Retention Policy* name).

Exchange Online

- Record attributes, e.g., date/time, sender, and recipients, provide audit information.
- In addition, the Exchange *mailbox audit logging* feature is in addition to the Security and Compliance Center audit system, described above.
  - When *mailbox audit logging* for user, shared and resource mailboxes is enabled by the administrator, some mailbox actions taken by delegates and administrators are logged by default and some must be configured in order to be tracked in the audit log. For each audit log entry, the action taken, user, date and time of the action, and unique item identifier are tracked. (Audit enhancements for Group Mailboxes are planned for release in approximately July 2019.)
  - The table below lists the lifecycle actions that Cohasset asserts should be enabled, as pertinent to inputting and changing mailbox items, as required for a mailbox that retains regulated records.

Action	Description	Admin	Delegate[14]	Owner
Create	A calendar, contact, note or task item is created for the mailbox. Note: Creating an email message or mailbox folder is not tracked in the audit log. For audit information related to sending and receiving email messages, see the bullet below related to system managed metadata.	Enable	Enable	Enable
SendAs	A message was sent using the SendAs permission. This means another user sent the message as though it came from the mailbox owner.	Enable	Enable	Not applicable
SendOnBehalf	A message was sent using the SendOnBehalf permission. This means 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.	Enable	Enable	Not applicable
HardDelete	An item purged from the Recoverable Items folder.	Enable	Enable	Enable

- In addition, audit data related to inputting and changing record objects is retained as system-managed metadata, such as, create/send/receive date, sender, and recipient(s) (distribution lists of up to 10,000 users are expanded), and modify date (when an item is copied prior to storing changes made to the subject or other user-updatable attributes).

[14] An administrator who has been assigned the Full Access permission to a user's mailbox is considered a delegate user.

2.12.4 Additional Considerations

- Audit logging must be enabled in the Security and Compliance Center.
- For Exchange Online, *mailbox audit logging* must be configured for the actions identified in Section 2.12.3. This feature is available for user, shared, and resource mailboxes.
  - *Mailbox audit logging* is not available for group mailboxes (including group mailboxes used by Teams). Accordingly, if group mailboxes retain regulated records, alternative means of capturing auditable actions related to inputting and modifying record objects must be established. This includes system-managed metadata, which tracks *when* an action is taken (e.g., create, send, and/or receipt date) and *what* action is taken (e.g., create or send an email, task, calendar entry, etc.). Note that *who* takes the action will be the group mailbox and not the specific user.
  - To maximize audit trail for *shared* mailboxes, individual users should be mailbox delegates; and, the role of mailbox owner should remain with the administrator. Note: Mailbox delegates may access the shared mailbox through Outlook, similar to their individual user mailbox.

2.13 Availability of Audit System for Examination

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

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

> **SEC 17a-4(f)(3)(v)(A):** 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.

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 audit log activities needed for compliance *supports* the regulated entity's efforts to access, download, store and provide the regulator with the requested audit system data.

Note: Audit activities are retained for a minimum of 90 days. For audit activities outside the availability period, this requirement to provide audit results must be satisfied by exports from the client's security information event management tool or other solution that retains the audit data; see Section 2.14, *Preservation of Audit Results*.

2.13.3 Capabilities of Assessed Office 365 Services

- The availability of the audit system data is dependent on the features to create and capture audit activities, as described in Section 2.12, *Audit System*.
- Audit results are retained, by default, for 90 days. During the availability period, authorized users may search, retrieve and export audit log activities using the Security and Compliance Center or Office 365 Management APIs
- Audit results older than 90 days must be retrieved and downloaded from the solution used by the regulated entity to preserve the audit logs. (See Section 2.14, *Preservation of Audit Results*.)
- The regulated entity must provide the audit results requested for examination.

2.13.4 Additional Considerations

- The regulated entity is responsible for (a) enabling audit logging, as described in Section 2.12, *Audit System*, (b) preserving the exported audit activities, as described in Section 2.14, *Preservation of Audit Results*, (c) conducting searches to locate requested audit log activities, (d) printing, downloading or otherwise producing audit log activities, in the requested format and medium, and (e) providing the produced audit results 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)]

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

It is Cohasset's opinion that the capabilities for searching and exporting audit log activities needed for compliance *support* the regulated entity's efforts to comply with this requirement to retain audit results, related to inputting and changing regulated records, for the same period of time as the associated record.

2.14.3 Capabilities of Assessed Office 365 Services

- Audit logging must be enabled; see Section 2.12, *Audit System*.
- Office 365 audit results are retained for a minimum of 90 days. During the availability period, using the Security and Compliance Center or the Office 365 Management APIs, authorized users must retrieve and export the audit log activities required for compliance with the Rule.
- Additionally, before a mailbox is designated as *inactive*, the mailbox audit folder must be exported, as it is *not* included when an *inactive* mailbox is restored.
- The regulated entity must import the audit results into its security information event management tool or other solution.
- Using separate tools, the regulated entity must retain the audit results in its solution for the time required for the audited records.

2.14.4 Additional Considerations

- The regulated entity is responsible for:
  - Exporting audit log activities from Office 365 during the availability period and then importing the audit log data into a security information event management tool or other solution.
  - Exporting mailbox audit log activities before the mailbox is designated as *inactive*.
  - Retaining the audit log activities in a security information event management tool or other solution for the required retention period.

- Due to the extensive volume of audit log activities in Office 365, which exceeds the requirements of the Rule, Cohasset suggests that the regulated entity carefully plan its process for exporting and preserving audit information for compliance with the Rule.

2.15 90-Day Notification and Compliance Representation

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

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

SEC 17a-4(f)(2)(i): The member, broker, or dealer 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 technology (including CD-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, the member, broker, or dealer must provide its own representation or one from the storage medium vendor or other third party with appropriate expertise that 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 Assessed Office 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, 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 maintain, keep current, and provide promptly upon request by the staffs of the Commission or the self-regulatory organizations of which the member, broker, or broker-dealer is a member all information necessary to access records and indexes 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 on the electronic storage media and the source code, together with the appropriate documentation and information necessary to access records and indexes.

2.16.2 Compliance Assessment

Cohasset asserts that Microsoft meets this SEC requirement by maintaining documentation on the Security and Compliance Center, Exchange Online, and the hardware and software used to access the records and properties and metadata attributes (index information) by offering technical support, as needed.

2.16.3 Capabilities of Assessed Office 365 Services

- The Security and Compliance Center and Exchange Online are cloud-based services, which store data in Microsoft data centers. Microsoft maintains the infrastructure necessary for authorized users to access the records and properties and metadata attributes (index information).
- Through TechNet articles, blogs and other resources, Microsoft publishes readily-available documentation on the features of Office 365, including methods of accessing records and associated properties and metadata attributes (index information).
- 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. Further, the regulated entity is responsible for managing and using its encryption keys that have been used in addition to the Customer Key service.

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, to assure access to the records and metadata attributes (index information).

In the event that Microsoft no longer provides access to the Office 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.

Additionally, for compliance with CFTC requirements, the regulated entity must keep an up-to-date inventory of systems associated with compliance. Specifically, 17 CFR § 1.31(c)(iii) requires:

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.

2.17 Designated Third Party Requirement

2.17.1 Compliance Requirement [SEC 17a-4(f)(3)(vii)]

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.*

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

The undersigned hereby undertakes to furnish promptly to the U.S. Securities and Exchange Commission ("Commission"), its designees or representatives, any self-regulatory organization of which it is a member, or any State securities regulator having jurisdiction over the member, broker or dealer, upon reasonable request, such information as is deemed necessary by the staffs of the Commission, any self-regulatory organization of which it is a member, or any State securities regulator having jurisdiction over the member, broker or dealer to download information kept on the broker's or dealer's electronic storage media to any medium acceptable under Rule 17a-4.

Furthermore, the undersigned hereby undertakes to take reasonable steps to provide access to information contained on the 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 broker or dealer pursuant to Rules 17a-3 and 17a-4 under the Securities Exchange Act of 1934 in a format acceptable to the staffs of the Commission, any self-regulatory organization of which it is a member, or any State securities regulator having jurisdiction over the member, broker or dealer. Such arrangements will provide specifically that in the event of a failure on the part of a broker or dealer to download the record into a readable format and after reasonable notice to the broker or dealer, upon being provided with the appropriate electronic storage medium, the undersigned will undertake to do so, as the staffs of the Commission, any self-regulatory organization of which it is a member, or any State securities regulator having jurisdiction over the member, broker or dealer may request.

2.17.2 Compliance Assessment

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

2.17.3 Capabilities of Assessed Office 365 Services

- Obtaining Designated Third-Party services are the responsibility of the broker-dealer.
- Microsoft may:
  - Enter into a designated third-party relationship with the broker-dealer,
  - Provide the necessary representation of its undertaking, and
  - Act as the third party who will promptly take reasonable steps to provide the regulated entity's records and index data that is stored in Exchange Online, as requested by the SEC or designated examining authority.

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 evaluation of the assessed capabilities of the Security and Compliance Center and Exchange Online, in comparison to the CFTC requirements.

The individual relevant requirements cited in Section 2, *Assessment of Compliance with SEC Rule 17a-4(f)*, are based on the wording in SEC Rule 17a-4(f) and Cohasset's interpretation of the requirements, given the associated SEC Interpretive Releases. Specifically, the SEC's 2003 Interpretive Release reiterates that the Rule sets forth standards that the electronic storage media must satisfy to be considered an acceptable method of storage under 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 assessed capabilities of the Security and Compliance Center and Exchange Online 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 the assessed features of the Security and Compliance Center and Exchange Online 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 the assessed capabilities of the Security and Compliance Center and Exchange Online, 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 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] It is Cohasset's opinion that Exchange Online retains properties and metadata 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 attributes, include but are not limited to, the unique identifier, creation (storage) date and time. For Exchange Online, the To, CC, BCC and From names and subject are also immutable. (A change to a subject causes a new version to be stored.) • Mutable (changeable) properties and metadata 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 the Security and Compliance Center and Exchange Online related to the authenticity and reliability of **indexes**. The Security and Compliance Center and Exchange Online includes an audit trail of actions taken and provides a method of exporting the audit trail so that it may be retained for the same time period as the electronic record. See Sections 2.12 through 2.14 for capabilities related to the authenticity and reliability of the **audit trail**.	**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 paragraph (f) as required by the Commission or the self-regulatory organizations of which the member, broker, or dealer is a member.* [SEC 17a-4(f)(2)(ii)(D)] ***Section 2.8 Organization and Accuracy of Indexes*** *Organize and index accurately all information maintained on both original and any duplicate storage media.* [SEC 17a-4(f)(3)(iv)] ***Section 2.11 Preservation of Indexes*** *Original and duplicate indexes must be preserved for the time required for the indexed records.* [SEC 17a-4(f)(3)(iv)(C)] ***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.* [SEC 17a-4(f)(3)(v)] ***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.* [SEC 17a-4(f)(3)(v)(A)] ***Section 2.14 Preservation of Audit Results*** *The audit results must be preserved for the time required for the audited records.* [SEC 17a-4(f)(3)(v)(B)]

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[15] 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 the replication and data resiliency features of Exchange Online, as described in Sections 2.7 and 2.10, meet the CFTC requirements (c)(2)(ii) to *ensure the availability of such regulatory records in the event of an emergency or other disruption of the records entity's electronic record retention systems*.	***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.* [SEC 17a-4(f)(3)(iii)] ***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.* [SEC 17a-4(f)(3)(iv)(B)] ***Section 2.14 Preservation of Audit Results*** *The audit results must be preserved for the time required for the audited records.* [SEC 17a-4(f)(3)(v)(B)]
(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 **paper** regulatory records*. *** (3) *Production of **electronic** regulatory records*. (i) A request from a Commission representative for electronic regulatory records will specify a *reasonable form and medium* in which a records entity must produce such regulatory records. (ii) A records entity must *produce such regulatory records in the form and medium requested promptly*, upon request, unless otherwise directed by the Commission representative. *(4) Production of **original** regulatory records.* ***	It is Cohasset's opinion that the capabilities described in the following sections support the regulated entity's efforts to comply with the CFTC requirements for *inspection and production of regulatory records stored electronically.* Specifically, it is Cohasset's opinion that: • 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 trail. Further, as noted in the *Additional Considerations* in Sections 2.4, 2.6, 2.9, and 2.13, the regulated entity is obligated to produce and provide the records, index and audit trail (respectively) in the form and medium requested.	***Section 2.4 Capacity to Download Indexes and Records*** *Have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable under this paragraph (f) as required by the Commission or the self-regulatory organizations of which the member, broker, or dealer is a member.* [SEC 17a-4(f)(2)(ii)(D)] ***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.* [SEC 17a-4(f)(3)(i)] ***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.* [SEC 17a-4(f)(3)(ii)] ***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*

[15] 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
		self-regulatory organizations of which the broker or dealer is a member. [SEC 17a-4(f)(3)(iv)(A)] ***Section 2.11 Preservation of Indexes*** *Original and duplicate indexes must be preserved for the time required for the indexed records.* [SEC 17a-4(f)(3)(iv)(C)] ***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.* [SEC 17a-4(f)(3)(v)(A)]

4 | Conclusions

Cohasset assessed the capabilities of Exchange Online, together with selected features of the Security and Compliance Center, in comparison to the requirements set forth in SEC Rule 17a-4(f) and its associated Interpretive Releases. As enumerated in the *Assessment Scope*, which begins Section 2, this assessment pertains to records stored and managed by Exchange Online, which is a cloud-based service that retains and manages mailbox items and certain archived items from Skype for Business Online and Microsoft Teams.

Cohasset determined that Exchange Online, together with certain features of the Security and Compliance Center, 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 Policies,* with *Preservation Lock,* which establishes 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, *locking* the policy provides integrated controls that *prevent* shortening the retention period of the policy and removing the policy from a record. When appropriately configured, the retention period assigned to the retention policy cannot be shortened and the retention policy cannot be removed from a record, after it is applied.
- 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 Security and 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 post-recording integrity verifications. When an error is detected, an accurate replica of the record is recovered or regenerated.
- Capturing the creation or receipt date and time 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 attributes (index information) and providing for recovery or regeneration of both the record and index information.
- Capturing properties and metadata attributes (index information) 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 Exchange Online mailboxes and Public Folders. Additionally, Teams Channel Messages, Teams Chats and Skype for Business conversations are organized chronologically.
- Allowing authorized users to readily sort and filter records using properties and metadata attributes (index information), and then download selected records and properties and metadata attributes (index information) to a medium acceptable under the Rule.

- Providing authorized users with robust content search tools to query the properties and metadata attributes (index information) stored for each record. These tools and search capabilities include full-text searches and keyword searches with a broad range of search conditions.
- 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 attributes.
- Generating human-readable renditions of the stored records in standard formats, except that the Teams Channel Messages and Teams Chats are stored as conversation segments, which must be manually connected. Further, weblinks are stored for emojis, giffies (GIFs), memes and stickers.
- Retaining system-managed metadata attributes to support audit requirements for inputting and changing records, in addition to retaining a comprehensive audit trail log, based on current and *planned* capabilities, and providing tools to export the audit log for the regulated entity to retain in 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 Exchange Online, together with selected features of the Security and Compliance Center, meet the non-rewriteable, non-erasable (WORM) requirement by applying *Compliance Retention Policies* (with *Preservation Lock*) and *eDiscovery Holds* to stored records. Further, the assessed features of the Security and Compliance Center and Exchange Online (together with the *planned* enhancements for an audit system, see Sections 2.12 and 2.13) meet or support the regulated entities' efforts to achieve compliance with the other requirements of the Rule. Further, Cohasset concludes that the capabilities of Exchange Online and the Security and Compliance Center meet the principles-based requirements of CFTC Rule 1.31(c)-(d).

5 | Overview of Relevant Regulatory Requirements

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

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

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

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

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

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

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

> ***SUMMARY:*** *The Securities and Exchange Commission ("Commission") is amending its broker-dealer record preservation rule to allow broker-dealers to employ, under certain conditions, electronic storage media to maintain records required to be retained. The amendments reflect a recognition of technological developments that will provide economic as well as time-saving advantages for broker-dealers by expanding the scope of recordkeeping options while at the same time continuing to require broker-dealers to maintain records in a manner that preserves their integrity. The Commission is also issuing an interpretation of its record preservation rule relating to the treatment of electronically generated communications.*
>
> ***
>
> ***II. Description of Rule Amendments***
> ***A. Scope of Permissible Electronic***
> ***Storage Media***
>
> ****The Commission is adopting a rule today which, instead of specifying the type of storage technology that may be used, sets forth standards that the electronic storage media must satisfy to be considered an acceptable method of storage under Rule 17a–4. Specifically, because optical tape, CD–ROM, and certain other methods of electronic storage are available in WORM and can provide the same safeguards against data manipulation and erasure that optical disk provides, the final rule clarifies that broker-dealers may employ any electronic storage media that meets the conditions set forth in the final rule.*[16] [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.

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).

[16] 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 17a-4 or other applicable Commission rules. Accordingly, a broker-dealer must take appropriate steps to ensure that records are not deleted during periods when the regulatory retention period has lapsed but other legal requirements mandate that the records continue to be maintained, and the broker-dealer's storage system must allow records to be retained beyond the retentions periods specified in Commission rules.* [emphasis added]

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

See Section 2, *Assessment of Compliance with SEC Rule 17a-4(f),* for a list of each SEC electronic records storage requirement and a description of the assessed capabilities of the Security and Compliance Center and Exchange Online 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 Electronic Regulatory Records Requirements

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

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

To address the transition to electronic regulatory records, the CFTC amended and modernized its recordkeeping regulation to adopt principles-based standards that are less prescriptive. This resulted in rephrasing and modernizing the requirements previously defined in 1999, as explained in the August 28, 2017, Federal Register in *III. Final Rules, D. Regulation 1.31(c): Form and Manner of Retention*:

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

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

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

These definitions establish that recordkeeping obligations apply to (a) all *records entities*, without exception, and (b) all *regulatory records*. Further, for *electronic regulatory records*, paragraphs (i) and (ii) establish an expanded definition of an electronic regulatory record to include information describing data necessary to access, search and display 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:*
>
> *(1) A records entity shall keep regulatory records of any swap or related cash or forward transaction (as defined in § 23.200(i) of this chapter), other than regulatory records required by § 23.202(a)(1) and (b)(1)-(3) of this chapter, from the date the regulatory record was created until the termination, maturity, expiration, transfer, assignment, or novation date of the transaction and for a period of not less than five years after such date.*
>
> *(2) A records entity that is required to retain oral communications, shall keep regulatory records of oral communications for a period of not less than one year from the date of such communication.*
>
> *(3) A records entity shall keep each regulatory record other than the records described in paragraphs (b)(1) or (b)(2) of this section for a period of not less than five years from the date on which the record was created.* [emphasis added]

For a list of the CFTC principles-based requirements and a summary assessment of the capabilities of the Security and Compliance Center and Exchange Online, in relation to each requirement, see Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*.

About Cohasset Associates, Inc.

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

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

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

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

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.