Cohasset Associates

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

Microsoft Azure Blob Storage

Abstract

Microsoft Azure Blob Storage is a cloud-based service, available on the Microsoft Azure Cloud platform, which provides large-scale storage for multiple types of data, including Blobs, Files, Queues, Tables and Disks.

For Azure Blob Storage, the *Immutable Storage* feature, with the *Policy Lock* option, is designed to meet securities industry requirements for preserving records in a non-rewriteable, non-erasable format. Each Blob (record) is protected from being modified, overwritten or deleted until the required retention period has expired and any associated legal holds have been released.

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

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

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

BENEFIT FROM COHASSET'S INDUSTRY INSIGHT AND EXPERIENCE

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

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

Table of Contents

1 | Introduction

Regulators, world-wide, establish explicit requirements for regulated entities that elect to retain books and records[1] on electronic storage media. Given the prevalence of electronic books and records, these requirements apply to most broker-dealer and commodity futures trading firms and other organizations with similarly regulated operations.

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

1.1 Overview of the Regulatory Requirements

1.1.1 SEC Rule 17a-4(f) Requirements

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

> *The Commission is adopting a rule today which, instead of specifying the type of storage technology that may be used, sets forth standards that the electronic storage media must satisfy to be considered an acceptable method of storage under Rule 17a–4.*[2] [emphasis added]

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

For additional information, refer to Section 5.1, Overview of SEC Rule 17a-4(f) Electronic Records Storage Requirements.

1.1.2 FINRA Rule 4511(c) Requirements

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

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

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

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

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

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

Refer to Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*, which correlates the CFTC principles-based requirements to the capabilities of Microsoft Azure Blob Storage. Additionally, refer to Section 5.3, *Overview of CFTC Rule 1.31(c)-(d) Electronic Regulatory Records Requirements*.

1.2 Purpose and Approach

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

Microsoft engaged Cohasset to:

- Assess the capabilities of Azure Blob Storage, utilized with the *Immutable Storage* feature and *Policy Lock* option, in comparison to the five requirements of SEC Rule 17a-4(f) for the recording and non-rewriteable, non-erasable storage of electronic records; see Section 2, *Assessment of Compliance with SEC Rule 17a-4(f);*
- Associate the principles-based requirements of CFTC Rule 1.31(c)-(d) to the assessed capabilities of Azure Blob Storage; 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.

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

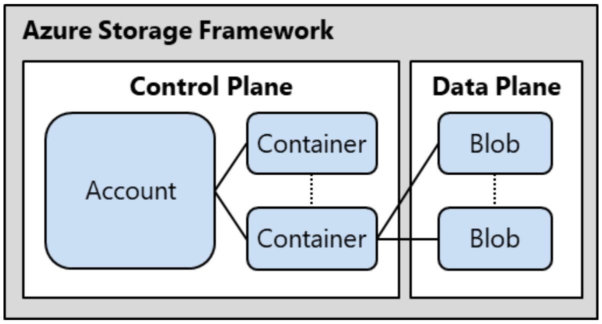
The content and conclusions of this assessment are not intended, and must not be construed, as legal advice. Relevant laws and regulations constantly evolve, and legal advice is tailored to the specific circumstances of the organization. Therefore, nothing stated herein should be substituted for the advice of competent legal counsel.

1.3 Azure Blob Storage Overview and Assessment Scope

The Azure Cloud platform is a comprehensive set of cloud services, hosted by Microsoft, which are designed for use by developers, IT professionals and Enterprises. One service available on the Azure platform is Azure Blob Storage, which provides large-scale storage for multiple types of data, including Blobs, Files, Queues, Tables and Disks. Azure Blob Storage, which is the focus of this assessment, allows customers to store large amounts of unstructured data, such as text or binary data, and access it from anywhere in the world. In addition, Azure Blob Storage can be extended with Azure Data Lake Storage Gen2 (ADLS Gen2) to provide hierarchical namespace, folder operations, and Access Control Lists (ACLs) per file or folder.

The Azure Blob Storage Framework consists of two conceptual components:

- **Control Plane** manages Storage Account and Container operations, including data organization, retention, and the application of immutability controls and legal hold tags.
  - A Subscription (client) on the Azure Cloud Platform utilizes Azure Storage Accounts, which are unique namespaces, to store and access Blobs (records).
  - Containers act as virtual file folders within an Account to organize the storage of Blobs (records).
    - Container names must be unique within an Account.
    - Containers have a single-level hierarchy, meaning they cannot hold other Containers, only Blobs (records).



- **Data Plane** manages data operations, such as reads, writes and deletes.

Azure defined two features for compliance with SEC Rule 17a-4(f) and other similar regulatory requirements to store Versioned Blobs (records) as non-rewriteable, non-erasable. While these two features are similarly named, the capabilities are considerably different. Throughout this report, Cohasset has specified either Immutable Storage or *Immutable Storage with Versioning*, to refer to each of these features :

- **Immutable Storage:** When an *Immutability Policy* is defined at the Container level, a mandatory retention interval is specified for the Container. Versioning may be enabled or disabled for the Container. The retention interval automatically applies to all Blobs or Versioned Blobs (records) retained within the Container and protects the Blobs or Versioned Blobs (records), and associated system and custom metadata, in a non-rewriteable and non-erasable format, for the duration of the retention period and any legal hold assigned to the Container. When the *Immutability Policy* is locked on a Container, via the *Policy Lock* option, stringent retention controls are applied, which prevent both shortening or removing the retention interval defined for the Container's *Immutability Policy*.
- **Immutable Storage with Versioning:** The *Immutability Policy with Versioning* feature requires *Versioning* to be enabled at the Account or Container level. Optionally, a default *Immutability Policy* (retention interval) and default *Policy Lock* status may be set for the Account and/or Container. When the *Policy Lock* status is locked, the *Immutability Policy* (retention interval) cannot be shortened, it can only be

lengthened.

The retention and immutability protections are optional settings for each Versioned Blob. When a retention expiration date is applied and the *Policy Lock* status is locked, the Versioned Blob (record) and associated system and custom metadata are protected, in a non-rewriteable and non-erasable format, until the version's retention expiration date has expired and the version’s Legal Hold attribute is off (“No”). Applying these stringent retention controls to a Versioned Blob (record) prevents both (a) shortening the retention expiration date and (b) changing the *Policy Lock* status of the Versioned Blob (record).

This assessment addresses Azure Blob Storage services *only* (including with Azure Data Lake Storage Gen2) and the specific features that are relevant for meeting the requirements of the SEC Rule. This assessment *excludes* Azure Storage services for Files, Queues, and Tables.

The following section documents Cohasset’s assessment of Azure Blob Storage, relative to the pertinent requirements in SEC Rule 17a-4(f).

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

This section presents Cohasset's assessment of the capabilities of Azure Blob Storage, utilized with the Immutable Storage features and the Policy Lock option, for compliance with the five requirements related to recording and non-rewriteable, non-erasable storage of electronic records, as stipulated in SEC Rule 17a-4(f).

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

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

The following subsections document Cohasset's assessment of the capabilities of Azure Blob Storage, as described in Section 1.3, *Azure Blob Storage Overview and Assessment Scope*, relative to each pertinent 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-rewriteable, non-erasable recording environment provided: (a) the storage solution delivers the prescribed functionality and (b) the functionality is delivered via appropriate integrated control codes for the SEC designated retention period associated with the stored records.

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

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

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

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

2.1.2 Compliance Assessment

It is Cohasset's opinion that the capabilities of Azure Blob Storage, with the *Immutable Storage* features and the *Policy Lock* option, meet this SEC requirement to retain records in non-rewriteable, non-erasable format for *time-based*[3] retention and any applied legal holds, when (a) properly configured, as described in Section 2.1.3 and (b) the considerations described in Section 2.1.4 are satisfied.

2.1.3 Azure Blob Storage Capabilities

This section describes the capabilities of Azure Blob Storage, utilized with the *Immutable Storage* features and the *Policy Lock* option, that directly pertain to this SEC requirement for preserving electronic records as non-rewriteable, non-erasable for the required retention period and any associated legal holds.

2.1.3.1 Protected Blob (Record) Definition

- A Blob (when versioning is disabled) or a Versioned Blob (when versioning is enabled) is a Protected Blob (record), while retention and immutability controls apply to it.
- Azure Blob Storage provides storage services for three types of Blobs:
  1. Block Blobs – used to hold ordinary files up to 200 TB in size.
     - Block Blobs may be written or copied to a Container.
  2. Page Blobs – used to hold random access files up to 8 TB in size.
     - Page Blobs must be created outside of a Protected Container, then copied to the Protected Container. *Note: Once retention and immutability controls are applied to a Page Blob Protected Container, further write operations are suspended.*
  3. Append Blobs – optimized for append operations, these are typically used for logging information.
     - Append Blobs are comprised of blocks of data sequentially added (appended) to the Blob. When Allow Append Blob is enabled for the container and an Append Blob is modified, all written content is immutable upon save and blocks are allowed to be added to the end of the Blob, via the

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

Append Block operation. Further details regarding the retention controls are described in the Append Blobs subsections of 2.1.3.3 and 2.1.3.4.

- A Protected Blob (record) is comprised of:
  - Complete content of the Blob or Versioned Blob.
  - Immutable metadata:
    - System metadata, including critical attributes such as Object ID (Blob name, Azure Data Lake Store Gen2 folder path, Container name, Account name), type of Blob, creation/storage date or Version ID (within Azure Blob Storage), checksums, encryption status, etc.
    - Custom metadata at the Blob (record) level, in the form of key value pairs, may include attributes such as search index values.
  - Mutable metadata:
    - Last modified date
    - Retention expiration date
    - Legal Hold attribute
    - Blob Index Tags
    - ADLS Gen 2 ACLs (Access Control List)
    - The storage tier utilized to store the Blob (record). Three storage tiers exist within the Azure Storage environment:
      - Hot – utilized for Blobs (records) requiring frequent access,
      - Cool – utilized when infrequent access is required,
      - Archive – appropriate when only limited access is necessary.

2.1.3.2 Summary of Immutable Storage and Immutable Storage with Versioning

Immutable Storage and *Immutable Storage with Versioning* are two separate Azure Blob Storage features designed for compliance with SEC Rule 17a-4(f), when the *Policy Lock* option is applied. These features store Protected Blobs (records) as non-rewriteable, non-erasable for time-based retention periods.

While these two features are similarly named, the capabilities are considerably different.

Summary of Immutable Storage

When a Container is configured for **Immutable Storage**:

1. A mandatory retention interval must be specified for the Container.
2. The *Lock Policy* option is enabled.
3. Up to ten (10) Legal Hold tags (Case ID) may be applied to the Container.
4. Versioning may be enabled or disabled for the Container.

The Container's retention interval and any legal holds automatically apply to all Protected Blobs (records) retained within the Container, assuring non-rewriteable and non-erasable format, for the duration of the retention period and any legal hold.

When the *Immutability Policy* is locked on a Container, via the *Policy Lock* option, stringent retention controls are applied, which prevent both shortening or removing the Container's retention interval.

Summary of Immutable Storage with Versioning

When an Account or Container is configured for **Immutable Storage with Versioning**:

1. Versioning must be enabled for the Account (which is inherited by each enclosed Container) or the Container.
2. An optional default retention interval and Policy Lock status may be specified for the Account and/or Container.
3. A retention expiration date and lock status, as well as the Legal Hold attribute (Yes/No), may be applied to each Versioned Blob (record).

When the *Immutability Policy* on the Account or Container is locked via the *Policy Lock* option (a) the *Immutability Policy* (retention interval) cannot be shortening and (b) the *Policy Lock* status cannot be changed to unlocked or removed.

The retention and immutability protections are optional settings for each Versioned Blob. Retention controls are either explicitly stipulated when the Versioned Blob is stored or are inherited from the Account or Container; further, the Legal Hold attribute may be set to Yes. If no retention or Legal Hold controls apply to the Versioned Blob, it is not protected. When a retention expiration date and Policy Lock status of locked are applied, the Versioned Blob (record) and associated system and custom metadata (record) are protected, in a non-rewriteable and non-erasable format, until the version's retention expiration date has expired and the version's Legal Hold attribute is off (“No”). Applying these stringent retention controls to a Versioned Blob (record) prevents both (a) shortening the retention expiration date and (b) changing the Policy Lock status of the Versioned Blob (record).

2.1.3.3 Immutable Storage - Configuration and Controls

- An Account with *Immutable Storage* enabled cannot have *Immutable Storage with Versioning*, as described in 2.1.3.4), enabled at the Account level.
- However, when a new Container is added to an Account with *Immutable Storage*, the new Container may be configured to utilize the *Immutable Storage with Versioning,* as described in Section 2.1.3.4, *Immutable Storage - Configuration and Controls*.

Container and Blob Configuration

- In Azure Blob Storage, the *Immutable Storage* features include an *Immutability Policy* (retention interval) and Hold tags (Case IDs) applied to a Container.
  - The *Immutability Policy* (retention interval), applied to a Container, may be *Locked* (hereinafter *Locked Immutability Policy*).

  - The *Immutability Policy* (retention interval) is stated as the number of days to retain past the Blob's (record's) creation/storage date or the last modified date[4], when allow protected appends is enabled on the Container. The *Immutability Policy* is used to *calculate* the retention expiration date for each Blob (record). The retention interval is <u>not</u> stored as part of the metadata for each Blob (record).
  - The *Immutability Policy* (retention interval) is configured through a two-step process:
    1. The Immutability Policy (retention interval) is set and stored at the Container level.
       - The retention interval is the number of *days* that each Blob (record) stored in the Container must be retained past its creation/storage date or past the last modified date (see footnote #4 when *allow protected appends* is enabled on the Container).
       - The retention expiration date for a Blob (record) is calculated, when needed, rather than stored as Blob (record) metadata.
       - Only one retention interval can be assigned to each Container.
       - As soon as the Immutability Policy is applied to a Container, immutability controls are applied to Blobs (records) stored within the Container and remain in effect for the lifespan of the Blobs (records). **However, until the *Policy Lock feature* is applied, the retention interval may continue to be modified and the Immutability Policy may be cleared (deleted). If the Immutability Policy is cleared, all immutability controls are removed from the Container and stored Blobs (records).**
    2. A Container's Immutability Policy ***must be locked,*** via the *Policy Lock* feature, to assure stringent retention controls are applied, which prevent both shortening and removing the retention interval defined for the Container's Immutability Policy.
  - The retention interval may be <u>*extended*</u> up to five (5) times per Container, up to a maximum of 400 years. If the retention interval is extended:
    - The new retention interval applies retroactively to Blobs (records) currently stored in the Container, as well as new Blobs (records) added to the Container.
    - The new retention interval and effective date are stored as Container metadata.
- Legal Hold tags (Case IDs) applied to a Container.
  - Each Legal Hold tag must be unique.
  - Up to ten (10) Legal Hold tags may be applied to a Container.

[4] The retention interval is added to the Append Blob's last modified date, if *allowProtectedAppendWritesV1* is enabled on the container, and the retention interval is added to either the Append or Block Blob's last modified date, if *allowProtectedAppendWritesV2* is enabled on the container.

- A new Account with *Immutable Storage* can be configured with versioning either enabled or disabled. When versioning is enabled, the retention expiration date is separately *calculated* for each version of a Blob (record), based on its metadata, as described above.
- When an *Immutability Policy* is applied to a Container:
  - If versioning is enabled on the Account, the retention interval and associated immutability controls apply to each Versioned Blob (record) in the Protected Container. Further, *new versions* are allowed for Blobs (records) within the Protected Container.
  - If versioning is disabled on the Account, Blobs (records) versions previously stored within the Container are assigned the retention interval and associated immutability controls; however, *new versions* are disallowed.

Container and Blob Controls

- For *Immutable Storage* to be compliant with SEC regulations, a Blob (record) must be stored in a Protected Container with an appropriate retention interval, and, when appropriate, a Legal Hold tag must be applied to the Protected Container.
  - Once a Blob (record) is written to a Protected Container, the Blob (record) is protected against (a) changes to stored content[5], (b) overwrites[6], (c) moves to any other Container, (d) moves to any other folder in ADLS Gen2, (e) creation of snapshots, (f) deletes, until the calculated retention expiration date has passed, and (g) renaming of the file path or of any folder in the container in ADLS Gen2. Further, a Blob (record) is protected for its lifespan; therefore, a Blob (record) that is past retention will continue to be protected from changes and overwrites until deleted.
- The *Locked Immutability Policy,* calculated retention expiration date and Legal Hold tags serve as integrated control codes, designed to preserve Blobs (records) and associated system and custom metadata as non-rewriteable and non-erasable**.**
- Once *Immutable Storage* is enabled with a *Locked Immutability Policy*, the controls cannot be removed from the Container (hereinafter Protected Container).
  - A Storage Account cannot be deleted if it has one or more Protected Containers.
- The following safeguards apply to Protected Containers:
  - The Immutability Policy (retention interval) cannot be removed from the Protected Container.
  - The retention interval cannot be shortened.
  - A Blob (record) cannot be deleted from the Protected Container until the Blob's (record's) retention expiration date has passed.

[5] By default, Azure prevents changes to Blobs. If the allowProtectedAppendWritesV1 or allowProtectedAppendWritesV2 feature is enabled, data can be appended to a Blob.

[6] For a Container with *Immutable Storage*: (a) if versioning is not enabled overwrites are prohibited and (b) if versioning is enabled overwrites generate a new version.

  - The Protected Container cannot be deleted if it contains one or more Blobs (records) or if a Legal Hold tag is applied.

- A Blob stored in a Protected Container may be _copied_ to another Container.
  - The original Blob (record) will remain in the original Protected Container and be governed by the Immutability Policy and Legal Holds applied to the original Container.
  - The new copy of the Blob (record) will retain its original creation/storage date and last modified date; however, a new retention expiration date will be calculated using the retention interval (if any) of the new Container and any Legal Hold tags applied to the new Container will apply.
- A Blob (record) stored in a Protected Container cannot be _moved_ to another Container.
- Blobs (records) may be moved between storage tiers throughout their lifespan within Azure Blob Storage. The immutability controls will remain in effect for the Blob (record), regardless of which storage tier is selected, and immutable Blob (record) metadata, such as creation/storage date and last modified date will remain unchanged.

Append Blobs

- When either the *allowProtectedAppendWritesV1* or the *allowProtectedAppendWritesV2* feature is enabled for the Container, the Append Blob write operation applies an updated last modified date, and the retention interval is added to the updated last modified date to calculate the retention expiration date. (See Subsection 2.1.3.1, *Protected Blob (Record) Definition*, for additional details.)
  - When allowProtectedAppendWritesV1 is enabled on the container, the retention interval is added to the Append Blob's last modified date.
  - When allowProtectedAppendWritesV2is enabled on the container, the retention interval is added to either the Append or Block Blob's last modified date.
- However, the Legal Hold feature, described below, takes precedence over the Immutability Policy (retention interval) and the Legal Hold feature cannot be configured with the *allowProtectedAppendWritesV1* feature; therefore, Legal Holds require use of the *allowProtectedAppendWritesV2* feature.

Legal Holds

- Legal Hold tags (Case IDs) are set and stored at the **Container level** to preserve all Blobs (records) in the Container for purposes of subpoena, litigation, regulatory investigation, and other similar circumstances.
  - Each Legal Hold must be uniquely identified with a Legal Hold tag (Case ID) of 23 characters or less.
  - A maximum of ten (10) Legal Holds are allowed per Container.
- All Blobs (records) stored within a Container with a Legal Hold tag, including those written to a Container after the tag is applied, are protected against (a) changes to stored content[7], (b) overwrites, (c) moves to any other

[7] By default, Azure prevents changes to Blobs. If the AllowProtectedAppendWritesV2 feature is enabled, data can be appended to a Blob and immutability features apply after the append write is completed.

Container (d) moves to any other folder in ADLS Gen2, (e) snapshots, (f) deletes, and (g) renames in ADLS Gen2.

- A Legal Hold tag can exist at the Container level as an independent control for the enclosed Blobs (records) and, therefore, does not require the Container to also have an assigned Immutability Policy (*locked or unlocked*).
- A Legal Hold tag should be cleared from the Container when preservation is no longer required.
- When all Legal Hold tags are cleared, immutability controls for the Container and Blobs (records) are governed by the *Immutability Policy*.

Disposition/Deletion and Overwrite

- Blobs (records) and associated metadata are protected from premature deletion and become eligible for deletion when the following conditions are met:
  - The Blob's (record's) calculated retention expiration date is in the past.
  - All Legal Hold tags have been cleared from the Container.
- An overwrite of a Blob (record) is only allowed when the Container holding it has (a) no assigned Immutability Policy (*locked or unlocked*) and (b) no assigned Legal Hold tag.
- Deletion of a Protected Container is prohibited if it has one or more Blobs (records) or if a Legal Hold tag is applied.
- Deletion of an Account that has one or more Protected Containers is prohibited.

2.1.3.4 *Immutable Storage with Versioning - Configuration and Controls*

- An Account with *Immutable Storage with Versioning* enabled cannot utilize *Immutable Storage* controls, as described in Section 2.1.3.3, *Immutable Storage - Configuration and Controls*.

Account, Container and Versioned Blob Configuration

- For Azure Blob Storage, the *Immutable Storage with Versioning* feature, includes the following.
  1. Versioning must be enabled for the Account.
  2. The *Immutability Policy* (retention interval) may be defined for an Account or Container at creation. If defined, the *Policy Lock* status must be locked on the *Immutability Policy* (hereinafter *Locked Immutability Policy*).
     - The *Immutability Policy* (retention interval) for the Account or Container is stated as the number of days to retain past the Versioned Blob's (record's) creation/storage date or after an Append Blobs last modified date. These serve as default retention intervals. The *Policy Lock* status must be locked.
       - Only one retention interval can be assigned to each Account or Container.
       - The Immutability Policy ***must be locked,*** via the *Policy Lock* feature, to assure:

      - The retention interval cannot be *shortened* or removed.
      - The *Policy Lock* status cannot be changed from locked to unlocked and cannot be removed.
    - The Account and Container level *Immutability Policies* (retention intervals) and *Policy Lock* status are hierarchical. Therefore, if specified, the Container-level *Immutability Policy* and *Policy Lock* status take precedence over the Account-level *Immutability Policy* and *Policy Lock* status.
      - The calculated retention expiration date and *Policy Lock* status are stored as metadata for the Versioned Blob (record) unless an explicit retention expiration date and *Policy Lock* status are transmitted with the Blob.
  - If an *Immutability Policy* (retention interval) is not defined for both the Account and the Container, the source application must apply an explicit retention expiration date to a Versioned Blob and the *Policy Lock* status of locked to the Versioned Blob for it to be protected; otherwise, the Versioned Blob is written without retention protections.
- Accounts and Containers governed by *Immutable Storage with Versioning* allow Legal Hold attributes (Yes/No) to be set for each Versioned Blob (record) or the base Blob.
- Accounts governed by *Immutable Storage with Versioning* cannot house Containers with *Immutable Storage* applied.

Account, Container and Versioned Blob Controls

- For *Immutable Storage with Versioning* feature to be compliant with SEC regulations, the Versioned Blobs (records) must be stored with a retention expiration date and *Policy Lock* status of locked. (These Versioned Blob controls may be explicitly transmitted with the Blob or inherited from the Container or Account defaults.) Additionally, a Legal Hold attribute must be applied to the Versioned Blob or the base Blob, when appropriate.
  - Versioned Blobs (records) with the above controls are protected against (a) changes to stored content[8], (b) overwrites, (c) moves to any other Account, (d) moves to any other folder in ADLS Gen2, (e) creation of snapshots, (f) deletes, until the Versioned Blob's retention expiration date has passed and the Legal Hold status is set to No, and (g) renaming of a blob’s file path or any folder in the container in ADLS Gen2.
  - Further, a Versioned Blob (record) is protected for its lifespan; therefore, a Versioned Blob (record) that is past retention will continue to be protected from changes and overwrites until deleted.
- The source application may transmit a Versioned Blob with an explicit retention expiration date and *Policy Lock* status, which overrides the defaults of the Container and/or Account and applies the explicit retention interval and Lock status to the Versioned Blob.

[8] By default, Azure prevents changes to Blobs. If the AllowProtectedAppendWritesV2 feature is enabled, data can be appended to a Blob.

  - The explicit retention expiration date may be shorter than the default retention interval specified for the Account or Container *Immutability Policy*.
  - The *Policy Lock* status may be set to unlocked; however, Versioned Blobs with an unlocked *Policy Lock* status are <u>not</u> compliant with the Rule.

- Further, the source application may transmit a Versioned Blob and explicitly specify that <u>no</u> retention expiration date and *Policy Lock* status apply. These settings override the defaults of the Container and/or Account and the Versioned Blob is written without retention protections, therefore, the Versioned Blob is <u>not</u> compliant with the Rule.
- The *Immutability Policy with Versioning,* the retention expiration date, *Policy Lock* status of locked, and Legal Hold attribute, stored as metadata for each Versioned Blob (record), serve as integrated control codes, designed to preserve Versioned Blobs (records) and associated system and custom metadata as non-rewriteable and non-erasable. Additionally, the Legal Hold attribute may be applied to the base Blob as integrated control codes that protect all associated Versioned Blobs (records).
  - The *Policy Lock* status of locked cannot be removed or changed to unlocked and the retention expiration date cannot be shortened for a Versioned Blob (record).
  - A Versioned Blob (record) cannot be deleted until the retention expiration date is in the past and the Legal Hold attribute is No for the Versioned Blob (record) and its base Blob.
- Once *Immutable Storage <u>with Versioning</u>* is enabled for an Account (hereinafter a Locked Account), it cannot be disabled or removed from the Account.
  - A *Locked Immutability Policy* applied to either an Account or Container cannot be removed and the retention interval cannot be shortened and the Policy Lock status cannot be changed, after the *Immutability Policy* is locked.
  - A Storage Account cannot be deleted if it has one or more Containers with a *Locked Immutability Policy*.
  - A Container cannot be deleted if it has one or more Versioned Blobs.
- A Versioned Blob (record) with retention protections may be *<u>copied</u>* to another Container.
  - The original Versioned Blob (record) will remain governed by its retention expiration date and Legal Hold attribute.
  - The new copy of the Versioned Blob will retain its original creation/storage date and last modified date; however, any retention protections and Legal Hold attributes must be separately applied to the new copy.
- Versioned Blobs (records) may be moved between storage tiers throughout their lifespan within Azure Storage. The immutability controls will remain in effect for the Versioned Blob (record), regardless of which storage tier is selected, and immutable Blob (record) metadata, such as creation/storage date will remain unchanged.

Append Blobs

- When the *allowProtectedAppendWritesV2* feature is enabled for the Container, the Append Blob write operation calculates the new retention expiration date by subtracting the current system date and time from the date and time when the retention expiration date was previously set, and then adding that time interval to the current storage / append date and time. The newly calculated retention expiration date is stored in the Append Blob metadata. (See *2.1.3.1 – Blob (Record) Definition*, for more details.)

Legal Holds

- The Legal Hold attribute preserves Blobs (records) for purposes of subpoena, litigation, regulatory investigation, and other similar circumstances.
  - When setting a legal hold, the Legal Hold attribute may be applied to (a) a specific Versioned Blob (if explicitly stated) or (b) to the base Blob (most recent version), if a specific Versioned Blob is not stated.
  - Legal Hold attribute may be set to "Yes" (On) or "No" (Off) for a Versioned Blob or base Blob.
- The Legal Hold attribute of Yes may be applied to the Versioned Blob or to the base Blob to protect all of its versions. The Legal Hold attribute of Yes protects against (a) changes to stored content[9], (b) overwrites, (c) snapshots, (d) deletes However, the Append Blob write operation is allowed and the Append Blobs are protected by the legal hold, after completion of the Append Blob write operation.
- The Legal Hold attribute can be applied as an independent control for Blobs stored in a Container governed by *Immutable Storage <u>with Versioning</u>*. An Account or Container is not required to have an assigned *Immutability Policy* (retention interval) that is *locked or unlocked*.
- The Legal Hold attribute should be cleared (No) on the Versioned Blob or base Blob when preservation is no longer required.
- When all Legal Hold attribute is cleared (No), the Versioned Blob is governed by its applied retention controls.

Disposition/Deletion and Overwrite

- Versioned Blobs (records) and associated metadata are protected from premature deletion and become eligible for deletion when the following conditions are met:
  - The Versioned Blob's (record's) retention expiration date, stored in the metadata, is in the past.
  - Legal Hold attributes have been cleared ("No") from the Versioned Blob and base Blob.
- Attempts to overwrite a Versioned Blob (record) stores a new version.
- Deletion of a Container is prohibited if it has one or more Blobs.
- Deletion of an Account that has one or more Containers is prohibited.

2.1.3.5 Migration from Immutable Storage to Immutable Storage with Versioning

- An existing Container configured with *Immutable Storage* may be migrated to *Immutable Storage <u>with Versioning</u>*.

[9] By default, Azure prevents changes to Blobs. If the AllowProtectedAppendWritesV2 feature is enabled, data can be appended to a Blob and immutability features apply after the append write is completed.

- Prior to migration, Legal Hold tags (Case IDs) must be cleared from the Container and Versioning must be enabled for the Account.
- The previously configured Container's *Immutability Policy* (retention interval) becomes the default *Immutability Policy* (retention interval). Therefore, new Blobs (records) written during migration will be assigned Versioned Blob protections, based on the Container's *Immutability Policy* (retention interval). However, new versions for existing Blobs cannot be written until migration is completed.
  - An Account-level default *Immutability Policy* (retention interval) is disallowed, since it can only be configured for Storage Accounts created at the same time that the *Immutable Storage with Versioning* feature is enabled.
- During migration, metadata stored for each Versioned Blob includes both (a) the Version ID (commit date/time stamp) and (b) the calculated retention expiration date.
- Post migration, the *Immutable Storage with Versioning* feature is enabled for the Container, even though the Account does not have this feature enabled.
- Additionally, after migration, Legal Holds must be applied to Versioned Blobs, as needed. As a reminder, the container-level Legal Hold tags (Case IDs) are no longer applicable.
- A Container with *Immutable Storage with Versioning* feature enabled cannot be reverted back to a Container with *Immutable Storage*. See Section *2.1.3.4, Immutable Storage with Versioning - Configuration and Controls,* for additional information.

2.1.3.6 Clock Management

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

2.1.3.7 Security

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

2.1.4 Additional Considerations

To assure compliance with the non-rewriteable, non-erasable requirements of the SEC Rule, the regulated entity is responsible for the pertinent activities described in the following three subsections.

2.1.4.1 *Immutable Storage* Considerations

- Applying an *Immutability Policy*, with an appropriate retention interval, and applying ***Policy Lock***, to every Container that is used to store regulated Blobs (records) either at the time the Container is created or within 24 hours of storing Blobs (records) in the Container. If Blobs (records) to be stored have multiple retention periods, the regulated entity must either (a) configure and use different Containers, each with an appropriate retention interval or (b) configure a single Container with a retention interval that is set to the longest retention period associated with the Blobs (records).
- Applying Legal Hold tags (Case IDs) to Containers with Blobs (records) that require preservation for legal matters, government investigations, external audits and other similar circumstances, and clearing the Legal Holds when no longer applicable.
  - Assigning descriptive, but not confidential, Legal Hold Case IDs, as the Case IDs are exposed.

- Since Legal Holds apply to all Blobs (records) in a Container, Cohasset also recommends that the regulated entity contemplate the type of Blobs (records) stored in each Container to limit excessive preservation of Blobs (records).
- The *allowProtectedAppendWritesV1* feature cannot be utilized with the Legal Hold feature, therefore, Cohasset recommends using only the *allowProtectedAppendWritesV2* feature.

2.1.4.2 Immutable Storage with Versioning Considerations

- Enabling *Immutable Storage with Versioning* and Versioning at Account creation.
- Applying an appropriate retention expiration date and Lock status to each Versioned Blob (record).
  - Cohasset recommends applying a default *Immutability Policy*, with an appropriate default retention interval, and applying *Policy Lock* for every Container (set either at the Account or Container level) that is used to store regulated Versioned Blobs (records) required for compliance.
  - Further Cohasset recommends that unprotected Versioned Blobs be stored in Containers without an *Immutability Policy* with the *Policy Lock* feature. (Note: Azure Blob Storage allows protected and unprotected Versioned Blobs to be commingled in a single Container.)
- Transmitting an *explicit* (user-defined) retention expiration date for regulated Versioned Blobs that are required to retained longer than the default *Immutability Policy* (retention interval).
- Applying the Legal Hold attribute of Yes to each Versioned Blob that require preservation for legal matters, government investigations, external audits, and other similar circumstances, and clearing the Legal Hold attribute when no longer applicable.

2.1.4.3 Further Considerations

- When version-level *Immutable Storage* features are needed, migrating Containers from an *Immutability Policy* to an *Immutability Policy with Versioning*.
- Ensuring all records required to be retained for compliance with the SEC Rule are uploaded to a properly configured Azure Blob Storage Container within 24 hours of creation or are stored in an SEC-compliant storage solution until uploaded to Azure Blob Storage.
- Establishing appropriate security policies and procedures to:
  - Restrict access to the Azure Storage Account Owner role.
  - Define the actions of the Azure Storage Account Owner.
  - Ensure appropriate levels of encryption is enabled for Blobs (records) at rest and in transit.
  - Periodically verify Microsoft's (and those of the regulated entity, where applicable) security/privacy/compliance audit results and/or certification reports.
- Ensuring that all security measures provided by a Data Trustee (in the event Sovereign Cloud Hosting is utilized) are consistent with the security measures provided by Microsoft within the Azure Storage environment.

- Storing Blobs (records) requiring event-based retention periods in a separate compliance system, since Azure Blob Storage does *not* currently support event-based retention periods.

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

2.2 Accurate Recording Process

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

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.

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

2.2.2 Compliance Assessment

Cohasset affirms that the capabilities of Azure Blob Storage, in conjunction with the inherent capabilities of advanced electronic recording technology, meet this SEC requirement for accurate recording and post-recording verification.

2.2.3 Azure Blob Storage Capabilities

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

Recording Process

- When a Blob (record) is uploaded to Azure Blob Storage:
  - The Blob (record) is divided into separate increments, i.e., blocks, that are written to the Azure Blob Storage environment.
  - As blocks of data are written, Azure Blob Storage automatically generates two secondary copies across different nodes of storage, for a total of three replicas.
  - A checksum is calculated for each block and stored as immutable metadata, at the individual block level, for post-recording verification.
  - Once Azure Blob Storage verifies that all three replicas have been successfully written and are identical, acknowledgement of a successful write is returned to the client. If a write failure occurs at any stage, an error message is returned to the invoking application for corrective action and the write operation is stopped to prevent corrupted data from being written to Azure Blob Storage.
  - Azure Blob Storage then utilizes erasure coding to finalize the write, which provides an automated method of error recovery that improves data durability and optimizes the storage space utilized.

- A customer may optionally provide a check-sum with a Blob (record) during the upload process.
  - If a *block-level* checksum is provided, it will be utilized by Azure Blob Storage to validate the recording process and will be stored as metadata.
  - If a *blob-level* checksum is provided, it will *not* be used to validate the storage process; instead, the checksum will be stored as metadata and may be accessed by the customer for independent checksum validation.
- Azure Blob Storage utilizes advanced electronic recording technology which applies a combination of checks and balances, such as inter-component and inter-step cyclical redundancy checks (CRCs) and write-error detection and correction, to assure that Blobs (records) are written in a high quality and accurate manner.

Post-Recording Verification Process

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

2.2.4 Additional Considerations

Cohasset recommends that the regulated entity:

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

2.3 Serialize the Original and Duplicate Units of Storage Media

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

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

SEC 17a-4(f)(2)(ii)(C): Serialize the 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

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

2.3.2 Compliance Assessment

It is Cohasset's opinion that the capabilities of Azure Blob Storage meet this SEC requirement to serialize the original and duplicate Blobs (records).

2.3.3 Azure Blob Storage Capabilities

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

2.3.4 Additional Considerations

There are no additional considerations related to this requirement.

2.4 Capacity to Download Indexes and Records

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

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

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

2.4.2 Compliance Assessment

It is Cohasset's opinion that Azure Blob Storage meets this SEC requirement to readily to download selected Blobs (records) and metadata (index) attributes, when the considerations described in Section 2.4.4 are addressed.

2.4.3 Azure Blob Storage Capabilities

- Azure Blob Storage capabilities that support the capacity to download Blobs (records) and associated metadata include:
  - Direct searches, via REST APIs (application programming interfaces), are allowed across the superset of system properties and metadata, e.g., Container name, retention interval, Policy Lock Status, Object ID

(Account/Container/Blob name), creation/storage date, last modified date and user ID. Search results can be saved to a separate database or downloaded to a media of choice.

  - Azure Search is a separate Azure Cloud platform service which reads through system and custom metadata, of both Containers and Blobs (records), to create an index which can then be saved to any database, e.g., MySQL, Cosmos DB, etc.
  - Third-party search tools may be utilized to search system and custom metadata, for both Containers and Blobs (records), to create an index which can then be saved to a separate database of choice.

- Once a search has identified desired Blobs (records), REST APIs may be used to retrieve a copy for transfer to any other compliant storage media.
- Microsoft further supports access to Blobs (records) by ensuring the Azure Storage environment maintains high availability, and proper capacity, based on the storage tier selected. Published availability numbers can be found at https://azure.microsoft.com/en-us/support/legal/sla/storage/v1_3/

2.4.4 Additional Considerations

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

2.5 Duplicate Copy of the Records Stored Separately

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

The intent of this requirement is to provide an alternate 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* is defined as a persistent copy that allows the complete and accurate record to be reestablished from data stored on a compliant storage system or medium. Whereas, a *backup copy* is defined as a non-persistent copy that is overwritten as it is *rotated* on a periodic basis, resulting in a much shorter retention period than the original.

2.5.2 Compliance Assessment

Cohasset asserts that Azure Blob Storage meets this SEC requirement for a persistent duplicate copy of the Blobs (records) when properly configured, as described in Section 2.5.3.

2.5.3 Azure Blob Storage Capabilities

- Azure Blob Storage provides four options for replicating Blobs (records):
  1. **Locally Redundant Storage (LRS)** – Three copies of all data are made synchronously across separate fault and upgrade domains within a single facility. This is the default method of replication within Azure Storage.

2. **Geo-Redundant Storage (GRS)** – Three LRS copies of the data are written synchronously to the primary data facility, then asynchronously, three more copies of the data (GRS) are written to a remote facility. The regulated entity does not have read access to the GRS data, as it exists for recovery purposes only.
3. **Read-Access Geo-Redundant Storage (RA-GRS)** – This alternate version of GRS grants the regulated entity with read access to the data stored in the secondary data center.
4. **Zone Redundant Storage (ZRS)** – This alternate replication option is available for Block Blobs only. Data is replicated synchronously across two to three *facilities*, within a single region or across two separate regions. This type of geographically separate replication offers more durability than LRS.

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

2.5.4 Additional Considerations

There are no additional considerations related to this requirement.

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

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

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

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

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

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

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

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

The focus of Cohasset's assessment, presented in Section 2, pertains to Azure Blob Storage, when the retention interval or retention expiration date is locked, which is a highly restrictive configuration that assures the storage solution applies controls to (a) protect immutability of the record content and certain system metadata,(b) prevent shortening or removing the retention expiration date and (c) prevent deletion over the applied retention period and any applied legal hold.

In the following table, Cohasset correlates the capabilities of Azure Blob Storage, when using a highly restrictive locked configuration, to the *principles-based* CFTC requirements related to the *form and manner of retention* and the *inspection and production of regulatory records*. In addition, Cohasset contends that the *Immutable Policy* (retention interval) feature does not need the *Policy Lock* feature to meet these *principles-based* CFTC requirements, when the regulated entity applies appropriate procedural controls to oversee operations that may allow a retention period to be shortened or content to be deleted prior to expiration of the retention period. This less restrictive (unlocked) *Immutable Policy*, provides flexibility to remove or shorten retention periods, which may be beneficial for compliance with privacy and data protection requirements.

The left-hand column lists the *principles-based* CFTC requirements. The middle column provides Cohasset's analysis and opinion regarding the ability of Azure Blob Storage to meet the requirements for electronic regulatory records in CFTC Rule 1.31(c)-(d). In addition, for ease of reference, the right-hand column lists the correlated SEC requirements.

CFTC 1.31(c)-(d) Requirement	Compliance Assessment Relative to CFTC 1.31(c)-(d)	SEC 17a-4(f) Requirements Listed in the Referenced Sections
(c) Form and manner of retention. Unless specified elsewhere in the Act or Commission regulations in this chapter, all regulatory records must be created and retained by a records entity in accordance with the following requirements: (1) **Generally**. Each records entity shall retain regulatory records in a form and manner that ensures the *authenticity and reliability* of such regulatory records in accordance with the Act and Commission regulations in this chapter. (2) **Electronic regulatory records**. Each records entity maintaining electronic regulatory records shall establish appropriate systems and controls that ensure the *authenticity and reliability* of electronic regulatory records, including, without limitation: (i) Systems that *maintain* the security, signature, and data as necessary to ensure the *authenticity* of the information contained in electronic regulatory records and to monitor compliance with the Act and Commission regulations in this chapter;	It is Cohasset's opinion that Azure Blob Storage capabilities, utilized with the *Immutable Storage* feature and the *Policy Lock* option, as described in Sections 2.1 through 2.4 meet CFTC requirements (c)(1) and (c)(2)(i) for Blobs (records). Additionally, for *records stored electronically*, the CFTC has expanded the definition of *regulatory records* in 17 CFR § 1.31(a) to include metadata: *Regulatory records means all books and records required to be kept by the Act or Commission regulations in this chapter, including any record of any correction or other amendment to such books and records, provided that, with 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 Azure Blob Storage retains immutable metadata attributes (e.g., Object ID, create date/time and retention), as an integral part of either (a) the Container or (b) the Versioned Blob. The immutable metadata attributes are subject to the same retention protections as the associated Blob (record). To satisfy this requirement for other essential data related to how and when the Blobs (records) were created, formatted, or modified, the regulated entity must retain this data in a compliant manner.	**Section 2.1 *Non-Rewriteable, Non-Erasable Record Format*** Preserve the records exclusively in a non-rewriteable, non-erasable format **Section 2.2 *Accurate Recording Process*** Verify automatically the quality and accuracy of the storage media recording process **Section 2.3 Serialize the Original and Duplicate 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 ***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.

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[10] in accordance with this section, and *ensure the availability of such regulatory records in the event of an emergency or other disruption* of the records entity's electronic record retention systems; and	It is Cohasset's opinion that Azure Blob Storage capabilities described in Section 2.5, including four options for duplicating the Blobs (records), meet the CFTC requirements (c)(2)(ii) to *ensure the availability of such regulatory records in the event of an emergency or other disruption of the records entity's electronic record retention systems*. To satisfy this requirement for other essential data related to how and when the Blob (records) were created, formatted, or modified, the regulated entity must retain this data in a compliant manner.	***Section 2.5 Duplicate Copy of the Records Stored Separately*** *Store separately from the original, a duplicate copy of the record stored on any medium acceptable under §240.17a-4 for the time required*
(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 Azure Blob Storage has features that support the regulated entity's efforts to comply with requests for inspection or production of Blobs (records) and associated system metadata (i.e., index attributes). Specifically, it is Cohasset's opinion that Section 2.4, *Capacity to Download Indexes and Records*, describes use of Azure Blob Storage to retrieve and download the Blobs (records) and the system metadata retained by Azure Blob Storage. As noted in the *Additional Considerations* in Section 2.4.4, the regulated entity is obligated to produce the Blobs (records) and associated metadata, in the form and medium requested. If the regulator requests additional data related to how and when the Blobs (records) were created, formatted, or modified, the regulated entity will need to provide this information from appropriate source systems.	***Section 2.4 Capacity to Download Indexes and Records*** *Have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable under this paragraph (f) as required by the Commission or the self-regulatory organizations of which the member, broker, or dealer is a member*

[10] 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.

4 | Conclusions

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

Cohasset determined that Azure Blob Storage, when properly configured with the *Immutable Storage* or *Immutable Storage <u>with Versioning</u>* feature and the *Policy Lock* option, has the following capabilities which meet the regulatory requirements:

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

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

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 SEC Rules 17a-3 and 17a-4, when the system delivers the prescribed functionality. Specifically, SEC Rule 17a-4(f)(1)(ii) states:

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

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

> ***SUMMARY:*** *The Securities and Exchange Commission ("Commission") is amending its broker-dealer record preservation rule to allow broker-dealers to employ, under certain conditions, electronic storage media to maintain records required to be retained. The amendments reflect a recognition of technological developments that will provide economic as well as time-saving advantages for broker-dealers by expanding the scope of recordkeeping options while at the same time continuing to require broker-dealers to maintain records in a manner that preserves their integrity. The Commission is also issuing an interpretation of its record preservation rule relating to the treatment of electronically generated communications.*
>
> ***
>
> ***II. Description of Rule Amendments***
> ***A. Scope of Permissible Electronic***
> ***Storage Media***
>
> ****The 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.*[11] [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-rewriteable, non-erasable recording environment, if the system delivers the prescribed functionality and appropriate **integrated control codes** are in place. The 2003 Interpretive Release states:

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

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

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

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

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

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

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

See Section 2, *Assessment of Compliance with SEC Rule 17a-4(f),* for a list of the five SEC requirements relevant to the recording and non-rewriteable, non-erasable storage of electronic records and a description of the capabilities of Azure Blob Storage related to each requirement.

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

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

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

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

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

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

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

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

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

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

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

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

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

For a list of the CFTC principles-based requirements and a summary assessment of Microsoft Azure Blob Storage 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.

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

For domestic and international clients, Cohasset:

- *Formulates information governance implementation strategies*
- *Develops policies and standards for records management and information governance*
- *Creates clear and streamlined retention schedules*
- *Prepares training and communications for executives, the RIM network and all employees*
- *Leverages content analytics to improve lifecycle controls for large volumes of eligible information, enabling clients to classify information, separate high-value information and delete what has expired*
- *Designs and 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*

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.