Cohasset Associates

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

Google Cloud Storage (GCS)

Abstract

Google Cloud Storage ("GCS") is a cloud-based service for storing and accessing record objects on Google's infrastructure, as part of the Google Cloud Platform. The GCS Bucket Lock feature, in combination with other GCS capabilities, are designed to meet securities industry requirements for preserving record objects in a non-rewriteable and non-erasable format, by protecting each record object from being overwritten or erased until it has been stored for the applied retention period and legal holds.

This Report documents the assessment conducted by Cohasset Associates, Inc. ("Cohasset") of the capabilities of GCS relative to the electronic records storage, retrieval and management requirements of the:

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

It is Cohasset's opinion that GCS, when properly configured and used with Bucket Lock, meets the five storage-related requirements and supports the regulated entity in meeting the seventeen requirements of SEC Rule 17a-4(f) and the principles-based requirements of CFTC Rule 1.31(c)-(d).

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

BENEFIT FROM COHASSET'S INDUSTRY INSIGHT AND EXPERIENCE

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

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

Table of Contents

1 | Introduction

The Securities and Exchange Commission (SEC) defines rigorous and explicit requirements for regulated entities[1] *that elect to retain books and records*[2] *on electronic storage media. Additionally, effective August 28, 2017, the CFTC promulgated new principles-based requirements on the form and manner in which regulated entities retain and produce books and records, including provisions for electronic regulatory records.*

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

Google has enhanced its cloud-based service for storing record objects to support compliance with these stringent electronic records storage, retrieval and management requirements. To evaluate its compliance with SEC Rule 17a-4(f) and CFTC Rule 1.31(c)-(d), Google engaged Cohasset to complete an independent and objective assessment of the capabilities of GCS, with the Bucket Lock feature configured, relative to these requirements.

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

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.* [emphasis added]

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

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

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

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

1.1.2 FINRA Rule 4511(c) Requirements

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

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

1.1.3 CFTC Rule 1.31 Requirements

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

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

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

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

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

1.2 Purpose and Approach

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

Cohasset was engaged to:

- Assess the capabilities of GCS, with the Bucket Lock feature configured, in comparison to the seventeen electronic storage requirements of SEC Rule 17a-4(f); see Section 2, *Assessment of Compliance with SEC Rule 17a-4(f);*
- Associate the principles-based requirements of CFTC Rule 1.31(c)-(d) to the assessed capabilities of GCS, with the Bucket Lock feature configured; see Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d);* and
- Prepare this Assessment Report, enumerating the results of its assessment.

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

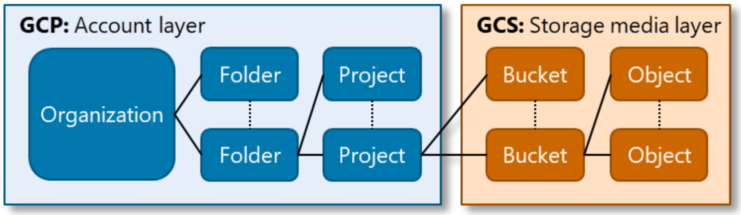
This assessment represents the professional opinion of Cohasset and should not be construed as either an endorsement or a rejection, by Cohasset, of GCS and its capabilities or other Google products or services. The information utilized by Cohasset to conduct this assessment consisted of: (a) oral discussions, (b) system documentation, (c) user and system administrator guides, and (d) other directly-related materials provided by Google 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 Google Cloud Storage (GCS)[3] Overview

Google Cloud Platform ("GCP") is hosted by Google and provides modular cloud-based products and services. Google Cloud Storage ("GCS") is one of the GCP services for developers and enterprises. GCS provides cloud-based virtual computers and a RESTful online object storage web service for storing and accessing objects on Google's infrastructure. As depicted in the graphic:

- **GCP** manages the *Account layer*. To facilitate account management activities, information resources with the Account are organized into Folders and Projects.
- **GCS** manages the *Storage media layer*, which contains Buckets that retain objects.



GCS stores objects in containers, referred to as GCS Buckets. The GCS Bucket Lock feature includes integrated control codes that were designed to enhance GCS features to meet the SEC Rule 17a-4(f) requirements, to preserve electronic record objects as non-rewriteable, non-erasable for the required retention period and any assigned legal holds.

[3] Throughout this Assessment Report, references to GCS pertain to Accounts with Buckets that are properly configured with the Bucket Lock feature and are used to store and retain immutable record objects.

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

This section presents Cohasset's assessment of the capabilities of GCS, with the Bucket Lock feature configured, for compliance with the seventeen requirements related to recording, storage, retention and management of electronic records, as stipulated in SEC Rule 17a-4(f).

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

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

The following subsections document Cohasset's assessment of the capabilities of GCS, with the Bucket Lock feature configured, relative to each requirement of SEC Rule 17a-4(f).

2.1 Non-Rewriteable, Non-Erasable Record Format

2.1.1 Compliance Requirement [SEC 17a-4(f)(2)(ii)(A)]

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

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

The following statement in the 2003 Interpretive Release further clarifies that certain implementations of rewriteable and erasable media, such as magnetic disk or magnetic tape, meet the requirements of a non-erasable and non-rewriteable recording environment provided: (a) the storage solution delivers the prescribed functionality, 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 current capabilities of GCS meet this SEC requirement, when (a) GCS Bucket features are properly configured and utilized to retain immutable record objects, (b) an appropriate fixed retention time period is applied to the Bucket and the retention policy locked, (c) flags for conditional (event-based) retention periods and legal holds are appropriately assigned to the record objects, and (d) the considerations identified in Section 2.1.4 are satisfied.

2.1.3 GCS Capabilities

In this section, Cohasset presents the current capabilities of GCS that directly pertain to the requirement for preserving electronic records (record objects) as non-rewritable and non-erasable, for the required retention period and any associated legal hold time periods.

General Information

An Account (client) on the Google Cloud Platform (GCP) uses GCS to store unstructured objects on Google's cloud infrastructure. Accordingly, GCP manages the *Account layer*, which is comprised of Projects and Folders, under which the GCS Buckets reside. GCS provides the *Storage media layer*, which manages the Buckets where the record objects are retained on the media.

The GCS Bucket Lock feature includes integrated control codes that were designed to preserve electronic record objects as non-erasable and non-rewriteable for the required retention period and any assigned legal holds, to meet the requirements of the SEC Rule.

The actions of applying a retention period to a Bucket and locking it (i.e., configuring Bucket Lock*)*:

- Precludes the retention policy from being removed from a Bucket; prevents shortening of the applied retention period; and prevents a Bucket from being deleted, unless it is empty, as long as the associated Account layer services in GCP are not removed.
- Enforces immutability and prohibits deleting, overwriting or changing the record object, together with its immutable object metadata, until the record object is *eligible for deletion*. The phrase *eligible for deletion* means that *all* the following conditions are met:
    - The duration of the Bucket retention policy added to the record object *Creation (Storage) Date* has passed[4],

[4] This enforces time-based retention periods, which require the record object to be retained for a specified period of time from the date and time the file is created/stored.

- The *Event Hold*[5] is *false* and the duration of the Bucket retention policy added to the record object *Event Date*[6] has passed (if an *Event Date* has been stored for the record object)[7], and
- The *Temporary Hold* (for legal holds, etc.) is *false* for the record object.

These retention attributes protect record objects from being deleted, overwritten or changed by (a) user-initiated actions, via application program interface (API), Google Cloud Console user interface (UI) or command-line interface (CLI) and (b) configuration-initiated actions, such as object lifecycle management actions. For additional information, see the subsection entitled *Retention Policy*.

Record Object Definition and Controls

This Assessment Report and the following record object definition and controls pertain to record objects stored in GCS, when properly configured with the Bucket Lock feature.

- Each record object stored in GCS is comprised of:
  - Complete content of the record object. For record objects that include a signature, a digital signature may be stored as an integral part of the record object transmitted for storage, or a scanned image may include a signature.
  - Immutable record object metadata, e.g., record object name, generation, creation (storage) date and time, size, and object checksums.
  - Mutable record object metadata, e.g., *Event Hold* attribute, *Temporary Hold* attribute, and user-specified custom metadata tags.

    NOTE: The retention duration is not stored as metadata for each record object but is applied via the Bucket retention policy. Once the Bucket retention policy is locked (lock status set to *true*), the retention duration can only be increased, but cannot be reduced.
- The record object name must be unique within the Bucket where it is stored. If a new record object's name is _not_ unique:
  - If the record object is eligible for deletion, the existing record object will be deleted, and the new record object will be stored with a unique generation number.
  - If the record object is _not_ eligible for deletion, an error message will be reported through the Google Cloud Console. and the new record object will not be stored.
- A record object can be *copied* between Buckets, resulting in the creation of a new copy with its own unique metadata, including the assignment of a new creation date and time, based on the time the copy was stored.

[5] The *Event Hold* enforces the indefinite portion of an event-based retention period (e.g., the period of time until a specific event occurs (e.g., until a contract expires or until an employee terminates).

[6] The *Event Date* is the most recent date that the *Event Hold* was changed from *True* to *False*, which should be the date that the event occurred (e.g., the date the contract expired or the date an employee terminated). The *Event Date* will be null if the *Event Hold* was never changed from *True* to *False*.

[7] The *Event Hold* and *Event Date* enforce event-based or event-time-based retention periods, which require the record object to be retained indefinitely until a specified event occurs (e.g., a contract expires or an employee terminates), after which the record object must be retained for a fixed retention period (e.g., 6 additional years).

- A record object *cannot* be *moved* between Buckets, unless the record object is *eligible for deletion*. If the record object is *eligible for deletion*, the move results in deleting the record object in the existing location and creating a new record object in the new location, with new metadata, including generation number and creation date and time.
- While object versioning must be disabled for a Bucket before a retention policy is applied, versions may exist in the Bucket. These existing versions will be managed as a separate record object. Further, the ability to restore a record object to an older state (i.e., overwrite a current record object with a prior version) will be disabled and will result in an error.

Retention Policy

- For compliance with SEC Rule 17a-4(f), the Bucket retention policy must be ***locked*** (lock status set to *true*) to assure:
  - The associated fixed retention duration of the retention policy cannot be shortened, though it may be extended.
  - The retention policy cannot be removed from the Bucket.
- Before a retention policy is applied to a Bucket, object versioning must be disabled.
- A Bucket-level retention policy is comprised of:
  - The minimum fixed retention duration that the record objects in the Bucket must be retained. If the record objects stored in the Bucket have different retention requirements, the Bucket duration must be set to the longest retention period for all record objects to be stored in the Bucket.
  - The *default* value for the *Event Hold* attribute, which is a simple Boolean value that each record object inherits when it is created (stored) in the Bucket. It is:
    - Set to *False* for retention periods based on the creation-date; or,
    - Set to *True* for retention periods that are kept indefinitely, until an event occurs.

    Alternatively, this attribute may be set when or after the record object is stored.
  - The effective date of the retention policy is automatically set by GCS to the oldest record object creation date of the record objects being controlled by that policy.
    - When the retention policy is first configured, the effective date is the policy creation date.
    - Thereafter, if the fixed retention duration of a retention policy is extended, the effective date is the most recent of:
      - The prior effective date, if none of the previously written record objects have expired, or
      - The policy change date minus the full duration of the *prior* Bucket-level retention policy duration.
    - This results in setting the retention policy effective date to the oldest record object creation date of the record objects being controlled by that policy.

- For a time-based retention policy, which requires the record object to be retained for a specified period of time from the date and time the record object is created/stored:
  - The Bucket retention duration is added to the creation date of each record object to calculate the retention expiration date for the record object.
  - If the fixed duration of the retention policy is *extended*, it (a) applies retroactively to record objects currently stored in the Bucket, and (b) applies to new record objects added to the Bucket.
  - The record object content, together with its immutable object metadata, are protected from being deleted, overwritten, archived, or otherwise modified until the calculated retention expiration date has passed.
- For an event-based retention policy, which requires the record object to be retained for an indefinite period of time until an *event* occurs (e.g., until the customer account is closed) and thereafter for a fixed duration of time:
  - The *Event Hold* attribute is set to *true*, either by the *default* value assigned to the Bucket or via API calls. When set to *true,* it enforces immutability and prohibits deleting, overwriting or changing the record object.
  - When the *Event Hold* attribute is changed from *true* to *false* for a specific record object, the current date is stored as the record object's *Event Date* (i.e., release date of the *Event Hold*); and, the retention expiration date is calculated by adding the current Bucket-level fixed retention duration to the record object *Event Date*. The record object is protected as immutable and cannot be deleted, overwritten or changed until the calculated retention expiration date has passed.
    - The record object's *Event Date* (i.e., release date of the *Event Hold*) cannot be modified by any other process other than setting the *Event Hold* from *true* to *false*.
  - If an *Event Hold* attribute is changed from *false* to *true* for a specific record object, it will return to the indefinite retention status. (This process may be used if a closed customer account is reopened, for example.) The *true* value of the *Event Hold* attribute enforces immutability and prohibits deleting, overwriting or changing the record object

Legal Holds (Temporary Holds)

- The *Temporary Hold* is a simple true/false Boolean value for each stored record object, which can be set via API calls.
  - When the *Temporary Hold* flag is *true,* it enforces immutability and prohibits both overwrite and deletion of the record object until the hold is removed. Accordingly, this feature may be used to preserve a record object for subpoena, litigation, regulatory investigation and other special circumstances.
  - When the *Temporary Hold* is *false,* this attribute no longer mandates preservation of the record object; however *other controls* may continue to protect the record object from being changed, deleted, overwritten, archived, or otherwise modified.
- Optionally, the reason for applying the hold may be stored in custom metadata, though this is not required.

Deletion

- The record object content, together with its object metadata, are *eligible for deletion* when **all** of the following conditions are met:
  - The duration of the Bucket retention policy added to the record object creation (storage) date has passed,
  - The *Event Hold* is *false* and the record object's *Event Date* (i.e., release date of the *Event Hold*) added to the duration of the Bucket retention policy has passed (if an *Event Date* has been stored for the record object), and
  - The *Temporary Hold* (for legal holds, etc.) is *false* for the record object.
- While deletion is **not** required by the SEC Rule, record objects are *eligible for deletion*, when the above conditions are met. Deletion may be initiated by:
  - Users with sufficient permission, through the API, UI or CLI.
  - Object Lifecycle Management actions configured to delete record objects.

    NOTE: The deletion actions are successful only for record objects that are *eligible for deletion*.
- Deleting a Bucket with record objects is prohibited.
  - A locked retention policy applied to a Bucket cannot be removed, which means all record objects in the Bucket must have been *eligible for deletion* and deleted before the Bucket can be deleted.

Clock Management

GCS uses TrueTime, Google's globally synchronized clock, which keeps strong consistency across the clocks in its data centers and tracks a time interval with bounded time uncertainty that is guaranteed to contain the clock's actual time. TrueTime's bounded time uncertainty is expressed in milliseconds and is documented as varying about 1 to 7 milliseconds in the Google production environment, assuring that timestamps are accurate when the data and metadata were fully written.

Security

- Independent third-party audits of Google's infrastructure, services and operations are undertaken on a regular basis to verify security, privacy and compliance controls. More information is available at https://cloud.google.com/security/compliance
- Record objects and metadata are encrypted:
  - GCS currently performs all operations using transport-layer encryption (HTTPS) to protect against data leakage over shared networks.
  - GCS encrypts data at rest and automatically decrypts the data, to render it for use. GCS maintains the encryption key for data at rest. More information is available at https://cloud.google.com/security/encryption-at-rest/default-encryption/
  - The regulated entity may encrypt record objects prior to uploading to GCS. The regulated entity is responsible for maintaining its encryption keys.

2.1.4 Additional Considerations

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

- Applying and locking a Bucket-level retention policy that meets regulatory requirements, either when the Bucket is created or within 24 hours of storing record objects in the Bucket. (This requires disabling the Object Versioning policy, if it was previously configured.)
- Setting the *Event Hold* to *true* to retain record objects for the indefinite period of a conditional retention period, such as *while the customer account is open*, and setting the *Event Hold* to *false* when the condition/event has been met.
- Applying *Temporary Holds* to record objects that require preservation for legal matters, government investigations, external audits and other similar circumstances, and releasing the Temporary Holds when the applicable action is completed.
- Ensuring all record objects required to be retained for compliance with the SEC Rule are uploaded to a properly configured GCS Bucket within 24 hours of creation or are stored in an SEC-compliant protected storage system until they are uploaded to GCS.

Cohasset also urges the regulated entity to set the following types of Organization Policies at the organization, folder, or project level and configure the policy to inherit down through the hierarchy, to supplement compliance with the SEC Rule.

- Require Buckets to have an applied retention policy.
- Setup eligible retention policies, such that GCS Buckets under that organization, folder, or project must match one of the configured retention policies. This assures that the retention policies conform to internal requirements.
- Set the Organization Policies to inherit from the parent to assure that policies assigned to the higher organizational layers are applied to the Buckets.

  Important Note: Organization Policies are <u>*not*</u> applied retroactively and are <u>*only*</u> enforced when a new Bucket is created or the retention period on an existing Bucket is updated. Therefore, Organization Policies should be configured before Buckets are setup, or retention policies for existing Buckets must be manually updated, as needed.

Additionally, the regulated entity is responsible for maintaining their GCP *Account layer* (Organization, Folder and Project) and paying for appropriate services. Similar to decommissioning a datacenter, deleting a Project in the Account layer will delete Buckets and record objects, even if the record object is *not* eligible for deletion. As a safeguard:

- A *Lien* set at the Project level, that is inherited by the Buckets, will prohibit Bucket deletion.
- Assigning the authority to create Projects to a compliance administrator role and then delegating responsibility of day-to-day management to a separate IT system administrator, without the permission to delete the project, will prevent the IT system administrator from removing the Lien and deleting the Bucket.

2.2 Accurate Recording Process

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

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

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

2.2.2 Compliance Assessment

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

2.2.3 GCS Capabilities

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

Recording Process:

- As part of the record object upload process, the user application may submit a checksum. When a checksum is provided, the record object will only be stored if the checksum calculated by GCS for the record object matches the user-provided checksum. If it does not match, an error is reported to the user audit log and the object must be re-uploaded.
- When a record object is uploaded to GCS, a *success* response is sent to the user application. This also indicates that the record object has been replicated.
- GCS computes and then saves checksums in the record object metadata. The checksum is immutable and is read-only to external users. The checksum is used in the post-recording period to verify the integrity of the record object.
- GCS maintains integrity information at each component of the internal architecture.
- GCS utilizes advanced electronic recording technology which applies a combination of checks and balances to assure that record objects are written in a high quality and accurate manner.

Post-Recording Verification Process:

- GCS durability features validate the record object content and are designed to assure 99.999999999% durability, for all storage classes.
- When a record object is retrieved, if any part of the data is incorrect, the GCS durability features will recover or regenerate an accurate replica.

2.2.4 Additional Considerations

Cohasset recommends that the regulated entity calculate a checksum of the record object content and transmit the checksum as record object metadata for GCS to verify the integrity of the uploaded record object.

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 GCS meet this SEC requirement to serialize the original and duplicate record objects.

2.3.3 GCS Capabilities

- The Global Identifier, which serializes each record object is comprised of (a) the Bucket name, which is unique across the entire GCS namespace, (b) a record object name, which is unique within the Bucket, and (c) version or generation. Each of these attributes is immutable.
  - The record object name must be unique for the Bucket where it is stored.
  - If it is not unique, the record object will not be stored, and an error message will be reported through the Google Cloud Console.
- The creation (storage) date and time captured and stored with each record object in a Bucket is immutable for the duration of the retention period.
- The combination of the Global Identifier and the creation (storage) date and time provide a serialization of each record object 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 GCS meets this SEC requirement by: (a) maintaining hardware and software capacity and high data availability, and (b) providing LIST and GET API methods to readily download the record objects and metadata (index) attributes. These record objects and metadata (index) attributes can then be transferred, by the regulated entity, in the format and media requested for production.

2.4.3 GCS Capabilities

Record objects and metadata (index) attributes may be downloaded using the GCS API, CLI or Google Cloud Console UI. The following capabilities support the capacity to download record objects and metadata (index) attributes:

- GCS assures that hardware and software capacity allows for ready access to the record objects and metadata (index) attributes. Further, GCS maintains redundant storage media, network, and power to mitigate outages that would result in unavailability of data. At any given time, data availability ranges from 99.0% to 99.95% and is based on the Storage class selected by the regulated entity.

- With the API, CLI or UI, authorized users can (a) list or search the Bucket name, (b) list record objects in lexicographic order, (c) search the object name, and (d) download the record object and a text file containing the associated metadata (index) attributes to a designated storage location. Record object metadata (index) attributes, include:

  - Immutable Bucket metadata, e.g., Bucket name, creation date and time.

  - Mutable Bucket metadata, e.g., Bucket labels and the retention duration, which can be increased, but not reduced.

  - Immutable object metadata, e.g., object name, generation, creation (storage) date and time, size, and object checksums.

  - Mutable record object metadata, e.g., *Event Hold*, *Event Date*, *Temporary Hold* and user-specified metadata tags for record objects.

  - Calculated retention expiration date for record objects, if a retention policy applies.

2.4.4 Additional Considerations

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

2.5 Readable Projection or Production of Images for Examination

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

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

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

2.5.2 Compliance Assessment

It is Cohasset's opinion that GCS supports the regulated entity's compliance with this SEC requirement by unencrypting the record object using the GCS encryption key and providing the record object for a browser or other local tool to render it as a human-readable image.

2.5.3 GCS Capabilities

- GCS encrypts data at rest and automatically decrypts the data, as part of the process of rendering the data for use. GCS maintains the encryption key for data at rest.
- GCS LIST and GET API calls allow authorized users to download record objects.
- Once downloaded, a browser or other local capabilities may be used to render a human-readable projection or print of the record objects.

2.5.4 Additional Considerations

The regulated entity is responsible for (a) maintaining its account in good standing, (b) authorizing user access, (c) maintaining hardware and software to access GCS, (d) maintaining its encryption keys that have been used in addition to the GCS encryption key, and (e) having hardware and software to view or print the record object.

2.6 Reproduction of Images Provided to Regulators

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

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

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

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

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

2.6.2 Compliance Assessment

It is Cohasset's opinion that GCS supports the regulated entity in meeting this SEC requirement to provide regulators with reproductions of the record objects.

2.6.3 GCS Capabilities

- At any given time, data availability ranges from 99.0% to 99.95% and is based on the Storage class selected by the regulated entity.
- GCS encrypts data at rest and automatically decrypts the data, as part of the process of rendering the data for use. GCS maintains the encryption key for data at rest.
- GCS LIST and GET API calls allow authorized users to download record objects. Thereafter:
  - The record objects may be provided to the regulator.
  - A browser or other local capabilities may be used to render a human-readable print of the record objects, which may be provided to the regulator.

2.6.4 Additional Considerations

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

2.7 Duplicate Copy of the Records Stored Separately

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

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

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

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

2.7.2 Compliance Assessment

Cohasset believes that GCS meets this SEC requirement through erasure coding, which stores coded segments of the record object across multiple disks located in different power and network failure domains. In the event of an error, an accurate replica of the full record object can be regenerated.

2.7.3 GCS Capabilities

- Each Bucket is configured with a default storage class, which designates the replication services for record objects added to the Bucket.
  - Objects added to the Bucket use this default storage class unless specified otherwise.
  - Any changes to the storage class applies to record objects that are added day forward and will not apply retrospectively to record objects that are already in the Bucket.
  - Further, the API may (a) specify the storage class of individual record objects being added to a Bucket, or (b) change the storage class for a record object.
- All GCS storage classes are designed for 99.999999999% durability, achieved through erasure coding that stores data pieces redundantly across multiple disks located in different power and network failure domains. This assures that a replica of the record objects can be accurately regenerated from the erasure coded data even in the event of the simultaneous loss of two disks. Storage class options include:
  - **Multi-Regional Storage Class**, which is asynchronously geo-redundant across two or more regions, with geographic locations separated by at least 100 miles. A minimum of two replicas (an original and a duplicate) of each record object are retained.
  - **Regional Storage Class**, which is redundant across multiple availability zones, in addition to being redundant across multiple disks, power, and network failure domains.
  - **Nearline** and **Coldline Storage Class**, which are redundant across multiple disks, power, and network failure domains.
- Optionally, object lifecycle management may perform an *in-place* downgrade of an object's storage-class. This process does **not** change the record object content, its creation date and time, generation number, *Event Hold*, *Event Date* or temporary hold. Accordingly, these in-place downgrade requests do not conflict with retention policy and are allowed for record objects under retention controls.

- Duplicates and erasure coded data segments are retained for the time period designated by the applied retention policies.

2.7.4 Additional Considerations

There are no additional considerations related to this requirement.

2.8 Organization and Accuracy of Indexes

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

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

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

2.8.2 Compliance Assessment

It is Cohasset's opinion that GCS supports the regulated entity in meeting this SEC requirement by storing the Bucket and record object names and metadata (index) attributes (including custom name-value pairs that describe various object attributes) for the same period of time as the corresponding record object.

2.8.3 GCS Capabilities

- The record objects are organized by Bucket name and by record object name.
  - The Bucket name can only be assigned during its creation.
    - All Buckets are at one level and cannot be hierarchical or nested.
    - A Bucket may have multiple Bucket labels, which allow for Buckets to be grouped along with other GCP resources.
  - The record object name can only be assigned during its creation (storage).
    - The record object name may include slashes to make objects appear to be organized in a hierarchical structure.
    - For each record object, custom name-value pairs that describe various object attributes, may be stored.
    - Authorized users may list the Bucket contents in lexicographical order or list objects matching a given prefix.
- Record object metadata (index) attributes include:
  - Immutable object metadata, e.g., object name, generation, creation (storage) date and time, size, and object checksums.
  - Mutable object metadata, e.g., *Event Hold*, *Event Date*, *Temporary Hold* and user-specified metadata tags for record objects.

- Additionally, when object metadata is retrieved (via LIST or GET API calls) the response will include (a) the calculated retention expiration date, i.e., the earliest date when object deletion is allowed, if a retention policy applies to the object, (b) the *Event Hold* status (for the indefinite portion of the retention period, such as *while the customer account is open*), and (c) the *Temporary Hold* status (for legal holds, etc.). If the *Event Hold* status is *true*, the retention expiration date will be null, since it is cannot be calculated until the event occurs.

2.8.4 Additional Considerations

The regulated entity is responsible for assigning logical Bucket and record object names and other record object metadata (index) attributes.

Additionally, the regulated entity is responsible for storing and managing any *other* index or metadata needed to meet the requirements of the SEC Rule. (This may include index or metadata retained by the source application storing the data on GCS).

2.9 Availability of Indexes for Examination

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

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

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

2.9.2 Compliance Assessment

Cohasset believes that GCS supports the regulated entity in meeting this SEC requirement by maintaining hardware and software capacity and high data availability and by providing LIST and GET API methods to readily retrieve and download the record objects' metadata (index) attributes.

2.9.3 GCS Capabilities

- At any given time, data availability ranges from 99.0% to 99.95% and is based on the Storage class selected by the regulated entity.
- With the API, CLI or UI, authorized users can (a) list record objects in lexicographic order, (b) search the object name, and (c) download metadata (index) attributes as a text file to a designated storage location. Record object metadata (index) attributes, include:
  - Immutable object metadata, e.g., object name, generation, creation (storage) date and time, size, and object checksums.
  - Mutable object metadata includes *Event Hold*, *Event Date*, *Temporary Hold* and user-specified metadata tags for record objects.
- Record object metadata (index) attributes are retained for the lifespan of the associated record object.

- The calculated retention expiration date (i.e., the earliest date when object deletion is allowed) can also be listed.

2.9.4 Additional Considerations

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

2.10 Duplicate Copy of the Index Stored Separately

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

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

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

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

2.10.2 Compliance Assessment

Cohasset asserts that GCS meets this SEC requirement by erasure coding the metadata (index) attributes retained by GCS. Erasure coding stores data segments across multiple disks located in different power and network failure domains. In the event of an error, an accurate replica of the metadata (index) attributes retained by GCS can be regenerated.

2.10.3 GCS Capabilities

- All storage classes are designed for 99.999999999% durability, achieved through erasure coding that stores data pieces redundantly across multiple disks located in different power and network failure domains. This assures that a replica of the GCS metadata (index) attributes can be accurately regenerated from the erasure coded data even in the event of the simultaneous loss of two disks. See Section 2.7, *Duplicate Copy of the Records Stored Separately*, for a list of storage classes.
- Additionally, when the Multi-Regional Storage Class is used, the metadata (index) attributes are automatically replicated across a minimum of two geographic locations separated by at least 100 miles.
- Erasure coded data segments of the GCS metadata (index) attributes are retained for the same retention period as the associated record object.

2.10.4 Additional Considerations

There are no additional considerations related to this requirement for the metadata (index) attributes stored in GCS.

2.11 Preservation of Indexes

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

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

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

2.11.2 Compliance Assessment

Cohasset asserts that GCS meets this SEC requirement for the metadata (index) attributes that it maintains by storing the Bucket and record object names and metadata (index) attributes (including custom name-value pairs that describe various object attributes) for the same retention period as the corresponding record object.

2.11.3 GCS Capabilities

- Record object metadata (index) attributes are retained as erasure coded data segments for the lifespan of the associated record object.
- Record object metadata (index) attributes, include:
  - Immutable object metadata, e.g., object name, generation, creation (storage) date and time, size, and object checksums.
  - Mutable object metadata includes *Event Hold*, *Event Date*, *Temporary Hold* and user-specified metadata tags for record objects.

2.11.4 Additional Considerations

There are no additional considerations related to this requirement for the metadata (index) attributes stored in GCS.

2.12 Audit System

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

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

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

2.12.2 Compliance Assessment

When Data Access logs are enabled as a GCP service, Cohasset asserts that GCS, in conjunction with GCP, support efforts to meet this SEC requirement by creating an audit trail for (a) creating or storing record objects on GCS, and (b) storing authorized modifications to an object.

2.12.3 GCS Capabilities

- A key component of the audit system is the calculation and maintenance of the effective date of the retention policy, which is automatically set by GCS to the *oldest record object creation date that the policy assures has been retained for the full retention period of the policy*.
  - When the retention policy is first configured, the effective date is the policy creation date.
  - Thereafter, if the fixed retention duration of a retention policy is *extended*, the effective date is the most recent of (a) the prior effective date or (b) today's date minus the full duration of the *prior* Bucket-level retention policy duration. *This sets the date to the oldest record object creation date that the policy assures has been retained for the full duration of the policy*.
- In addition, the audit system utilizes Google Cloud Audit Logging, which is a GCP service that maintains Admin Activity logs and Data Access logs and makes the logs available for a period of time through the Google Cloud Console.
  - Admin Activity logs document operations that modify the configuration or metadata of a Project or Bucket. The attributes of the modification are *not* captured. Examples of captured operations include:
    - Creating and deleting Buckets.
    - Setting and changing Identity and Access Management (IAM) policies.
    - Updating Bucket metadata.
  - Data Access logs must be enabled. When enabled, the *Data Write* activity documents operations that create or modify an object. The attributes of the modification are *not* captured.
- The creation (storage) date and time of the record object is immutable and is retained for the lifespan of the record object.

2.12.4 Additional Considerations

The regulated entity is responsible for (a) retaining audit log activity (see Section 2.14., *Preservation of Audit Results*), and (b) capturing an audit trail of transactions initiated by the source system, for object-level activities that are *not* currently captured by GCP, if required for regulatory compliance. Examples of activities that are *not* captured include changes to the *Event Hold* and *Temporary Hold* attributes applied to objects.

2.13 Availability of Audit System for Examination

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

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

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

2.13.2 Compliance Assessment

When Data Access logs are enabled as a GCP service, Cohasset believes that GCS, in conjunction with GCP, support efforts to meet this SEC requirement to make the audit system available to the regulated entity for submission to the SEC or self-regulatory organization.

2.13.3 GCS Capabilities

- The Google Cloud Audit Logging is a GCP service that maintains Admin Activity and Data Access logs and makes the logs available for a period of time through the Google Cloud Console.
- Authorized system administrators for the regulated entity can use the GCP Google Cloud Audit Logging service to:
  - Search and filter for audit trail entries by:
    - *Audit Log Name:* Audit log entries belong to logs within projects and organizations.
    - *Resource:* Each audit log entry tracks the associated GCP resource.
    - *Service:* Services are individual products, such as Compute Engine, Cloud SQL, or Cloud Pub/Sub.
  - Export the selected audit trail events for the period of time retained in GCP.

2.13.4 Additional Considerations

The regulated entity is responsible for (a) capturing audit trail activity in GCP and in internal security information event management tools (see Section 2.14., *Preservation of Audit Results*), (b) conducting searches to locate requested audit trail data, (c) printing, downloading or otherwise producing audit trail data, in the requested format and medium, and (d) providing the produced audit trail data to the regulator, self-regulatory organization or designated examining authority.

2.14 Preservation of Audit Results

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

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

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

2.14.2 Compliance Assessment

When Data Access logs are enabled as a GCP service, Cohasset asserts that GCS supports efforts to meet this SEC requirement to retain the audit results for the same time period as the audited records.

2.14.3 GCS Capabilities

- The Google Cloud Audit Logging is a GCP service that maintains Admin Activity and Data Access logs and makes the logs available for a period of time through the Google Cloud Console.
- Authorized users must export the audit trail activities from the Google Cloud Audit Logging service to another solution. Options include:

- Configuring the automatic export of log entries to a GCS Bucket, with an appropriate retention policy. Optionally, setting lock status of the retention policy to *true*, which applies strict retention controls.
- Importing log entries into the regulated entity's internal (non-GCP) security information event management tool, and then use that tool and data to retain the audit trail events for the required retention period.

2.14.4 Additional Considerations

The regulated entity is responsible for (a) exporting audit trail events from GCP, during the period of time they are available, (b) capturing the audit trail for object-level activities initiated by source systems that are *not* currently captured by GCP, if required for regulatory compliance, (c) storing the audit trail for the required retention period.

2.15 90-Day Notification and Compliance Representation

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

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

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

2.15.2 Compliance Assessment

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

2.15.3 GCS Capabilities

- The regulated entity is responsible for notifying its designated examining authority at least 90 days prior to employing electronic storage media, other than optical disk technology, as required by this SEC Rule.
- This Assessment Report and other documentation may be provided to the regulated entity for preparation of its notification letter.

2.15.4 Additional Considerations

There are no additional considerations related to this requirement.

2.16 Availability of Information to Access Records and Indexes or Escrow

2.16.1 Compliance Requirement [SEC 17a-4(f)(3)(vi)]

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

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

2.16.2 Compliance Assessment

Cohasset asserts that GCS meets this SEC requirement by maintaining documentation on the hardware and software used to access the records and metadata (index) attributes and by offering technical support, as needed.

2.16.3 GCS Capabilities

- The GCS record objects and metadata (index) attributes reside in a cloud environment under the control of Google and are not kept on the premises of the regulated entity.
- Google maintains the GCS infrastructure necessary for authorized users to access the record objects and metadata (index) attributes.
- Administration of the solution is shared by GCS and enterprise administrators.
- GCS maintains the encryption keys it uses to encrypt data at rest.

2.16.4 Additional Considerations

The regulated entity is responsible for placing in escrow or otherwise making available its encryption keys that have been used, in addition to the GCS encryption key. to assure access to the record objects and metadata (index) attributes.

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

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

> *The creation and maintenance of an up-to-date inventory that identifies and describes each system that maintains information necessary for accessing or producing electronic regulatory records.*

2.17 Designated Third Party Requirement

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

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

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

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

> *The undersigned hereby undertakes to furnish promptly to the U.S. Securities and Exchange Commission ("Commission"), its designees or representatives, any self-regulatory organization of which it is a member, or any State securities regulator having jurisdiction over the member, broker or dealer, upon reasonable request, such information as is deemed necessary by the staffs of the Commission, any self-regulatory organization of which it is a member, or any State securities regulator having jurisdiction over the member, broker or dealer to download information kept on the broker's or dealer's electronic storage media to any medium acceptable under Rule 17a-4.*
>
> *Furthermore, the undersigned hereby undertakes to take reasonable steps to provide access to information contained on the broker's or dealer's electronic storage media, including, as appropriate, arrangements for the downloading of any record required to be maintained and preserved by the broker or dealer pursuant to Rules 17a-3 and 17a-4 under the Securities Exchange Act of 1934 in a format acceptable to the staffs of the Commission, any self-regulatory organization of which it is a member, or any State securities regulator having jurisdiction over the member, broker or dealer. Such arrangements will provide specifically that in the event of a failure on the part of a broker or dealer to download the record into a readable format and after reasonable notice to the broker or dealer, upon being provided with the appropriate electronic storage medium, the undersigned will undertake to do so, as the staffs of the Commission, any self-regulatory organization of which it is a member, or any State securities regulator having jurisdiction over the member, broker or dealer may request.*

2.17.2 Compliance Assessment

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

2.17.3 GCS Capabilities

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

2.17.4 Additional Considerations

There are no additional considerations related to this requirement.

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

The objective of this section is to document Cohasset's assessment of the capabilities of GCS, with the Bucket Lock feature configured, in comparison to the CFTC requirements.

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

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

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

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

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

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

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

CFTC 1.31(c)-(d) Requirement	Compliance Assessment Relative to CFTC 1.31(c)-(d)	SEC 17a-4(f) Requirements Listed in the Referenced Sections
(c) Form and manner of retention. Unless specified elsewhere in the Act or Commission regulations in this chapter, all regulatory records must be created and retained by a records entity in accordance with the following requirements: (1) Generally. Each records entity shall retain regulatory records in a form and manner that ensures the *authenticity and reliability* of such regulatory records in accordance with the Act and Commission regulations in this chapter. (2) Electronic regulatory records. Each records entity maintaining electronic regulatory records shall establish appropriate systems and controls that ensure the *authenticity and reliability* of electronic regulatory records, including, without limitation: (i) Systems that *maintain* the security, signature, and data as necessary to ensure the *authenticity* of the information contained in electronic regulatory records and to monitor compliance with the Act and Commission regulations in this chapter;	It is Cohasset's opinion that the capabilities of GCS, with the Bucket Lock feature configured, as described in Sections 2.1 through 2.4, meet CFTC requirements (c)(1) and (c)(2)(i) for record objects. 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 GCS, with the Bucket Lock feature configured, retains the immutable metadata (index attributes) as an integral part of record object; and, therefore these attributes are subject to the same retention protections as the associated record object. Immutable metadata, includes, but is not limited to the object name, generation, creation (storage) date and time, size, and object checksums. Additionally, GCS, with the Bucket Lock feature configured, retains mutable (changeable) metadata attributes for a record object, such as, *Event Hold* attribute, *Temporary Hold* attribute, and user-specified custom metadata tags. See Sections 2.8 and 2.11 for GCS capabilities related to the authenticity and reliability of indexes. GCS creates an audit trail of actions taken and provides a method of storing the audit trail for the same time period as the record object. See Sections 2.12 through 2.14 for capabilities related to the authenticity and reliability of the audit trail. To satisfy this requirement for other essential data that is not retained in GCS (such as separate indices), the regulated entity must retain this other data in a compliant manner.	Section 2.1 *Non-Rewriteable, Non-Erasable Record Format* *Preserve the records exclusively in a non-rewriteable, non-erasable format.* [SEC 17a-4(f)(2)(ii)(A)] Section 2.2 *Accurate Recording Process* *Verify automatically the quality and accuracy of the storage media recording process.* [SEC 17a-4(f)(2)(ii)(B)] Section 2.3 Serialize the Original and Duplicate Units of Storage Media *Serialize the original and, if applicable, duplicate units of storage media, and time-date for the required period of retention the information placed on such electronic storage media.* [SEC 17a-4(f)(2)(ii)(C)] *Section 2.4 Capacity to Download Indexes and Records* *Have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable under this paragraph (f) as required by the Commission or the self-regulatory organizations of which the member, broker, or dealer is a member.* [SEC 17a-4(f)(2)(ii)(D)] *Section 2.8 Organization and Accuracy of Indexes* *Organize and index accurately all information maintained on both original and any duplicate storage media.* [SEC 17a-4(f)(3)(iv)] *Section 2.11 Preservation of Indexes* *Original and duplicate indexes must be preserved for the time required for the indexed records.* [SEC 17a-4(f)(3)(iv)(C)] *Section 2.12 Audit System* *The member, broker, or dealer must have in place an audit system providing for accountability regarding inputting of records required to be maintained and preserved pursuant to §§240.17a-3 and 240.17a-4 to electronic storage media and inputting of any changes made to every original and duplicate record maintained and preserved thereby.* [SEC 17a-4(f)(3)(v)] *Section 2.13 Availability of Audit System for Examination* *At all times, a member, broker, or dealer must be able to have the results of such audit system available for examination by the staffs of the Commission and the self-regulatory organizations of which the broker or dealer is a member.* [SEC 17a-4(f)(3)(v)(A)] *Section 2.14 Preservation of Audit Results* *The audit results must be preserved for the time required for the audited records.* [SEC 17a-4(f)(3)(v)(B)]

CFTC 1.31(c)-(d) Requirement	Compliance Assessment Relative to CFTC 1.31(c)-(d)	SEC 17a-4(f) Requirements Listed in the Referenced Sections
(ii) Systems that ensure the records entity is able to produce electronic regulatory records[8] in accordance with this section, and *ensure the availability of such regulatory records in the event of an emergency or other disruption* of the records entity's electronic record retention systems; and	It is Cohasset's opinion that the GCS capabilities described in the following sections 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*. ● Sections 2.7 and 2.10 explain that all GCS storage classes are designed for 99.999999999% durability, achieved through erasure coding that stores data pieces redundantly across multiple disks located in different power and network failure domains. ● In Section 2.14.3 Cohasset explains a GCS Bucket may be populated with audit trail events. Data stored in a GCS Bucket is protected, as described in Sections 2.7and 2.10. To satisfy this requirement for other essential data that is not retained in GCS (such as separate indices), the regulated entity must retain this other data in a compliant manner.	*Section 2.7 Duplicate Copy of the Records Stored Separately* *Store separately from the original, a duplicate copy of the record stored on any medium acceptable under §240.17a-4 for the time required.* [SEC 17a-4(f)(3)(iii)] *Section 2.10 Duplicate Copy of the Index Stored Separately* *Each index must be duplicated and the duplicate copies must be stored separately from the original copy of each index.* [SEC 17a-4(f)(3)(iv)(B)] *Section 2.14 Preservation of Audit Results* *The audit results must be preserved for the time required for the audited records.* [SEC 17a-4(f)(3)(v)(B)]
(iii) The creation and maintenance of an *up-to-date inventory* that identifies and describes each system that maintains information necessary for accessing or producing electronic regulatory records.	The regulated entity is required to create and retain an *up-to-date inventory,* as required for compliance with 17 CFR § 1.31(c)(iii).	N/A

[8] 17 CFR § 1.31(a) includes indices (*Any data necessary to access, search, or display any such books and records*) in the definition of regulatory records.

CFTC 1.31(c)-(d) Requirement	Compliance Assessment Relative to CFTC 1.31(c)-(d)	SEC 17a-4(f) Requirements Listed in the Referenced Sections
(d) Inspection and production of regulatory records. Unless specified elsewhere in the Act or Commission regulations in this chapter, a records entity, at its own expense, must *produce or make accessible for inspection* all regulatory records in accordance with the following requirements: (1) *Inspection*. All regulatory records shall be open to inspection by any representative of the Commission or the United States Department of Justice. (2) *Production of paper regulatory records*. *** (3) *Production of electronic regulatory records*. (i) A request from a Commission representative for electronic regulatory records will specify a *reasonable form and medium* in which a records entity must produce such regulatory records. (ii) A records entity must *produce such regulatory records in the form and medium requested promptly*, upon request, unless otherwise directed by the Commission representative. *(4) Production of original regulatory records.* ***	It is Cohasset's opinion that the capabilities described in the following sections support the regulated entity's efforts to comply with the CFTC requirements for *inspection and production of regulatory records stored electronically.* Specifically, it is Cohasset's opinion that: ● Sections 2.4, 2.5, and 2.6, pertain to the inspection and production of record objects. ● Sections 2.4, 2.9 and 2.11 pertain to the inspection and production of indexes. ● Section 2.13 pertains to the inspection and production of the audit trail. Further, as noted in the *Additional Considerations* in Sections 2.4, 2.6, 2.9, and 2.13, the regulated entity is obligated to produce and provide the records, index and audit trail (respectively) in the form and medium requested. If the regulator requests additional data related to how and when the record objects 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.* [SEC 17a-4(f)(2)(ii)(D)] *Section 2.5 Readable Projection or Production of Images for Examination* *At all times have available, for examination by the staffs of the Commission and self-regulatory organizations of which it is a member, facilities for immediate, easily readable projection or production of micrographic media or electronic storage media images and for producing easily readable images.* [SEC 17a-4(f)(3)(i)] *Section 2.6 Reproduction of Images Provided to Regulators* *Be ready at all times to provide, and immediately provide, any facsimile enlargement which the staffs of the Commission, any self-regulatory organization of which it is a member, or any State securities regulator having jurisdiction over the member, broker or dealer may request.* [SEC 17a-4(f)(3)(ii)] *Section 2.9 Availability of Indexes for Examination* *At all times, a member, broker, or dealer must be able to have such indexes available for examination by the staffs of the Commission and the self-regulatory organizations of which the broker or dealer is a member.* [SEC 17a-4(f)(3)(iv)(A)] *Section 2.11 Preservation of Indexes* *Original and duplicate indexes must be preserved for the time required for the indexed records.* [SEC 17a-4(f)(3)(iv)(C)] *Section 2.13 Availability of Audit System for Examination* *At all times, a member, broker, or dealer must be able to have the results of such audit system available for examination by the staffs of the Commission and the self-regulatory organizations of which the broker or dealer is a member.* [SEC 17a-4(f)(3)(v)(A)]

4 | Conclusions

Cohasset assessed the capabilities of GCS, with the Bucket Lock feature configured, in comparison to the requirements 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 GCS.

Cohasset determined that GCS, with Bucket Lock, has the following capabilities, which meet the regulatory requirements:

- Retaining the record objects in a non-erasable, non-rewriteable format, by applying integrated control codes to manage time-based[9] and event-time-based[10] retention periods and legal holds. These retention controls prevent deleting, overwriting or changing a record object for the applied retention period.
  - The time-based retention policy is applied to a GCS Bucket and is locked.
  - The event-based retention attribute is applied to the record object using the *Event Hold* attribute.
  - The legal hold is applied to a record object by setting the *Temporary Hold* attribute.
- Verifying the accuracy and quality of the recording process through checksums and GCS validation processes, in addition to the inherent capabilities of advanced magnetic storage technology.
- Uniquely serializing each record object with an immutable Global Identifier.
- Retaining immutable metadata, such as the record object creation date and time and unique identifier for the full retention period of the record object.
- Regenerating an accurate replica of the record object and metadata (including index attributes) 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 power or network domain locations.
- Providing capacity and tools to (a) list record objects in lexicographic order, (b) search the object name, and (c) download the record object and associated metadata (index) attributes for a browser or other local tool to render a human-readable image.

Additionally, GCS supports the regulated entity's compliance with audit trail and index requirements. Audit trail entries must be exported from GCP, during the period of time they are available, and may be stored in a GCS Bucket or another tool for the required retention period. Additionally, the regulated entity may use other source applications and solutions to manage audit trail and index information.

Accordingly, Cohasset concludes that the GCS capabilities, when properly configured, including use of Bucket Lock, meet the five storage-related requirements and support the regulated entity in meeting the seventeen requirements of SEC Rule 17a-4(f) and the principles-based requirements of CFTC Rule 1.31(c)-(d).

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

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

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-erasable and non-rewriteable recording environment, if the system delivers the prescribed functionality and appropriate **integrated control codes** are in place. The 2003 Interpretive Release states:

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

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

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

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

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

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

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

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

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

See Section 2, *Assessment of Compliance with SEC Rule 17a-4(f),* for a list of each SEC electronic records storage requirement and a description of the capabilities of GCS 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 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 record objects, as well as information describing how and when such books and records were created, formatted, or modified.

The retention time periods for regulated records includes both time-based[12] and event-time-based[13] retention periods. Specifically, 17 CFR § 1.31 (b)(1)-(b)(3) states:

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

For a list of the CFTC principles-based requirements and a summary assessment of the capabilities of GCS, with the Bucket Lock feature configured, in relation to each requirement, see Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*.

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

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

About Cohasset Associates, Inc.

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

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

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

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

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

For domestic and international clients, Cohasset:

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

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

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