Cohasset Associates

Google Cloud Storage™

COMPLIANCE ASSESSMENT

SEC 17a-4(f), SEC 18a-6(e), FINRA 4511(c) and CFTC 1.31(c)-(d)

Abstract

Google Cloud Storage™ is a highly-flexible, managed service for storing and accessing unstructured data on Google Cloud infrastructure. The service combines the performance and scalability of Google Cloud with advanced security and sharing capabilities.

In this report, Cohasset Associates, Inc. (Cohasset) assesses the functionality of Google Cloud Storage (see Section 1.3, *Google Cloud Storage Overview and Assessment Scope*) relative to the electronic records requirements, specified by multiple regulatory bodies, as follows:

- Securities and Exchange Commission (SEC) in 17 CFR § 240.17a-4(f)(2);
- SEC in 17 CFR § 240.18a-6(e)(2);
- Financial Industry Regulatory Authority (FINRA) in Rule 4511(c), which defers to the format and media requirements of SEC Rule 17a-4(f); and
- Commodity Futures Trading Commission (CFTC) in 17 CFR § 1.31(c)-(d).

It is Cohasset's opinion that Google Cloud Storage, when properly configured and used with the *Retention* features in *locked* mode, has functionality that meets the electronic recordkeeping system requirements of SEC Rules 17a-4(f)(2) and 18a-6(e)(2) and FINRA Rule 4511(c), as well as supports the regulated entity in its compliance with SEC Rules 17a-4(f)(3) and 18a-6(e)(3). Additionally, the assessed functionality of Google Cloud Storage meets the principles-based requirements of CFTC Rule 1.31(c)-(d).

COHASSET'S INDUSTRY INSIGHT AND EXPERIENCE

Core to our practice is the delivery of records management and information governance professional consulting services, and education and training. Cohasset's expert consulting services support regulated organizations, including those in financial services. Cohasset serves both domestic and multi-national clients, aligning information lifecycle controls to their organizations' business priorities, facilitating regulatory compliance and risk mitigation, while generating quantifiable business efficiency.

Cohasset assesses a range of electronic recordkeeping systems, each designed to meet the requirements of the Securities and Exchange Commission Rules 17a-4(f)(2) and 18a-6(e)(2) for record audit-trail and non-rewriteable, non-erasable record formats, considering the SEC 2001, 2003 and 2019 interpretations. For the non-rewriteable, non-erasable record, these interpretations authorize the use of erasable storage, conditioned on integrated software or hardware control codes, to prevent overwriting, erasing, or otherwise altering the records, during the applied retention period.

December 2023

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

+1.312.527.1550 | www.cohasset.com

Table of Contents

Abstract **1**

Table of Contents **2**

1 • Introduction **3**

1.1 Overview of the Regulatory Requirements 3

1.2 Purpose and Approach 4

1.3 Google Cloud Storage Overview and Assessment Scope 5

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

2.1 Record and Audit-Trail 6

2.2 Non-Rewriteable, Non-Erasable Record Format 7

2.3 Record Storage Verification 19

2.4 Capacity to Download and Transfer Records and Location Information 21

2.5 Record Redundancy 22

2.6 Facilities to Produce Records for Examination 24

2.7 Provide Records to Regulators 25

2.8 Audit System 26

2.9 Information to Access and Locate Records 28

2.10 Designated Executive Officer or Designated Third Party Requirement 29

3 • Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d) **31**

4 • Conclusions **34**

Appendix A • Overview of Relevant Electronic Records Requirements **35**

A.1 Overview of SEC Rules 17a-4(f) and 18a-6(e) *Electronic Recordkeeping System* Requirements 35

A.2 Overview of FINRA Rule 4511(c) *Electronic Recordkeeping System* Requirements 37

A.3 Overview of CFTC Rule 1.31(c)-(d) *Electronic Regulatory Records* Requirements 38

Appendix B • Cloud Provider Undertaking **39**

B.1 Compliance Requirement 39

B.2 Google Undertaking Process 40

B.3 Additional Considerations 40

About Cohasset Associates, Inc. **41**

1 • Introduction

Regulators, worldwide, establish explicit requirements for certain regulated entities that elect to electronically retain books and records. Given the prevalence of electronic books and records, these requirements apply to most broker-dealers, commodity futures trading firms and similarly regulated organizations.

This Introduction *summarizes the regulatory environment pertaining to this assessment and the purpose and approach for Cohasset's assessment. It also provides an overview of Google Cloud Storage and the assessment scope.*

1.1 Overview of the Regulatory Requirements

1.1.1 SEC Rules 17a-4(f) and 18a-6(e) Requirements

In 17 CFR §§ 240.17a-3 and 240.17a-4 for the securities broker-dealer industry and 17 CFR §§ 240.18a-5 and 240.18a-6 for nonbank SBS entities[1], the SEC stipulates recordkeeping requirements, including retention periods.

Effective January 3, 2023, the U.S. Securities and Exchange Commission (SEC) promulgated amendments to 17 CFR § 240.17a-4 (SEC Rule 17a-4) and 17 CFR § 240.18a-6 (SEC Rule 18a-6), which define explicit requirements for electronic storage systems.

> *The Securities and Exchange Commission ("Commission") is adopting amendments to the recordkeeping rules applicable to broker-dealers, security-based swap dealers, and major security-based swap participants. The amendments modify requirements regarding the maintenance and preservation of electronic records****[2] [emphasis added]

For additional information, refer to Section 2, *Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e),* and Appendix A.1, *Overview of SEC Rules 17a-4(f) and 18a-6(e) Electronic Recordkeeping System Requirements*.

1.1.2 FINRA Rule 4511(c) Requirements

Financial Industry Regulatory Authority (FINRA) rules regulate member brokerage firms and exchange markets. These rules were amended to address security-based swaps (SBS).[3]

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

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

---

1 Throughout this report, 'nonbank SBS entity' refers to security-based swap dealers (SBSD) and major security-based swap participants (MSBSP) that are not also registered as a broker-dealer without a prudential regulator.

2 Electronic Recordkeeping Requirements for Broker-Dealers, Security-Based Swap Dealers, and Major Security-Based Swap Participants, Exchange Act Release No. 96034 (Oct. 12, 2022) 87 FR 66412 (Nov. 3, 2022) (2022 Electronic Recordkeeping System Requirements Adopting Release).

3 FINRA, Regulatory Notice 22-03 (January 20, 2022), FINRA Adopts Amendments to Clarify the Application of FINRA Rules to Security-Based Swaps.

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

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

For additional information, refer to Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*, and Appendix A.3, *Overview of CFTC Rule 1.31(c)-(d) Electronic Regulatory Records Requirements*.

1.2 Purpose and Approach

To obtain an independent and objective assessment of the compliance capabilities of Google Cloud Storage™ for preserving required electronic records, Google engaged Cohasset Associates, Inc. (Cohasset). As a specialized consulting firm, Cohasset has more than fifty years of experience with the legal, technical, and operational issues associated with the records management practices of companies regulated by the SEC and CFTC. Additional information about Cohasset is provided in the last section of this report.

Google engaged Cohasset to:

- Assess the functionality of Google Cloud Storage, in comparison to the electronic recordkeeping system requirements of SEC Rules 17a-4(f)(2) and 18a-6(e)(2) and describe features that support the regulated entity in its compliance with SEC Rules 17a-4(f)(3) and 18a-6(e)(3); see Section 2, *Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e);*
- Address FINRA Rule 4511(c), given FINRA explicitly defers to the requirements of SEC Rule 17a-4; see Section 2, *Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e);*
- Associate the principles-based requirements of CFTC Rule 1.31(c)-(d) with the assessed functionality of Google Cloud Storage; see Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d);* and
- Prepare this Compliance Assessment Report, enumerating the assessment results.

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

This assessment represents the professional opinion of Cohasset and should not be construed as either an endorsement or a rejection, by Cohasset, of Google Cloud Storage and its functionality 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) 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 Overview and Assessment Scope

1.3.1 Google Cloud Storage Overview

Google Cloud is hosted by Google and provides a global suite of cloud-based computing products and services. As one of the Google Cloud services, Google Cloud Storage provides cloud-based virtual computing services and a RESTful online object storage web service for storing and accessing unstructured data[4] on Google's infrastructure. Google Cloud Storage logical storage architecture is depicted in Figure 1:

- **Google Cloud** manages the *Account layer*. To facilitate account management activities, information resources for the Account are organized into Folders and Projects.
- **Google Cloud Storage** manages the *Storage layer* and stores objects in containers, referred to as Buckets.

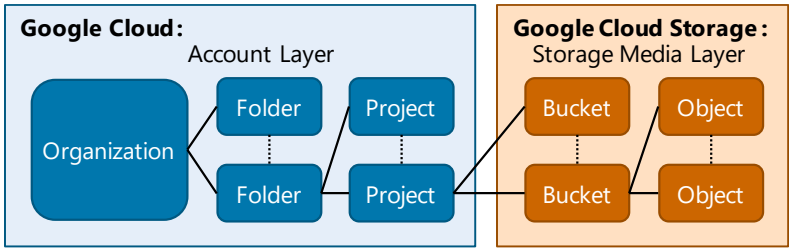

Figure 1: Google Cloud Storage Logical Storage Architecture

A Bucket that is intended to store records in a non-erasable and non-rewriteable format for a time-based[5] or event-based[6] retention period, must be configured for use with the *Retention* features, by enabling (a) Bucket Lock, (b) Object Retention Lock, or (c) both Bucket Lock and Object Retention Lock. Versioning is optionally available for use with Object Retention Lock and when enabled, retention controls are separately applied to each record version. The *Retention* features (Bucket Lock, Object Retention Lock, or a combination of both) utilized in *locked* mode are designed to meet the SEC Rule 17a-4(f) requirements to preserve electronic records as non-rewriteable, non-erasable for the required retention period and any assigned legal holds. Specifically, the *locked* mode assures the application of highly-restrictive, integrated retention controls that systemically disallow any users or administrators from shortening or removing retention controls.

1.3.2 Assessment Scope

The scope of this assessment is focused specifically on the compliance-related capabilities of Google Cloud Storage, when utilized with the *Retention* features in *locked* mode.

NOTE: Google Cloud Storage also offers a less-restrictive *unlocked* retention mode that provides flexibility for administrators to remove or shorten retention periods, which may be beneficial for compliance with privacy and other data protection requirements. However, for compliance with SEC Rules, in this report, Cohasset assesses the more stringent controls provided with *locked* retention mode.

---

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

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

6 Event-based retention periods require records to be retained indefinitely until a specified condition is met (e.g., a contract expires or an employee terminates), after which the record is retained for a fixed final retention period.

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

This section presents Cohasset's assessment of the functionality of Google Cloud Storage, for compliance with the electronic recordkeeping system requirements promulgated in SEC Rules 17a-4(f)(2) and 18a-6(e)(2), as well as describes how the solution supports the regulated entity in meeting the requirements of SEC Rules 17a-4(f)(3) and 18a-6(e)(3).

For each compliance requirement described in this section, this assessment is organized as follows:

- ***Compliance Requirement*** – Excerpt of relevant regulatory requirement in SEC Rules 17a-4(f) and 18a-6(e) and Cohasset's interpretation of the specific requirement
  - Both SEC Rules 17a-4(f) and 18a-6(e) are addressed in this section, since the electronic recordkeeping system requirements (principles, controls and testable outcomes) are the same, though the Rules specify their respective regulations and regulators and include semantic differences.
- ***Compliance Assessment*** – Summary statement assessing compliance of Google Cloud Storage
- ***Google Cloud Storage Capabilities*** – Description of assessed functionality
- ***Additional Considerations*** – Additional clarification related to meeting the specific requirement

The following sections document Cohasset's assessment of the capabilities of Google Cloud Storage, as described in Section 1.3, *Google Cloud Storage Overview and Assessment Scope*, relative to the enumerated requirements of SEC Rules 17a-4(f) and 18a-6(e).

2.1 Record and Audit-Trail

2.1.1 Compliance Requirement

This regulatory requirement, adopted with the 2022 Rule amendments, allows regulated entities to use a combination of electronic recordkeeping systems, with each system meeting either (a) the record and audit-trail requirement, as described in this section or (b) the non-rewriteable, non-erasable record format requirement, as explained in Section 2.2, *Non-Rewriteable, Non-Erasable Record Format*.

This record and audit-trail requirement is designed to permit use of the regulated entities' business-purpose recordkeeping systems to achieve the required outcome without specifying any particular technology solution.

SEC 17a-4(f)(2)(i)(A) and 18a-6(e)(2)(i)(A):

Preserve a record for the duration of its applicable retention period in a manner that maintains a complete time-stamped audit-trail that includes:

(1) All modifications to and deletions of the record or any part thereof;

(2) The date and time of actions that create, modify, or delete the record;

(3) If applicable, the identity of the individual creating, modifying, or deleting the record; and

(4) Any other information needed to maintain an audit-trail of the record in a way that maintains security, signatures, and data to ensure the authenticity and reliability of the record and will permit re-creation of the original record if it is modified or deleted

The SEC clarifies that this requirement to retain the record and its complete time-stamped audit-trail promotes the authenticity and reliability of the records by requiring the electronic recordkeeping system to achieve the testable outcome of reproducing the original record, even if it is modified or deleted during the required retention period, without prescribing how the system meets this requirement.

> *[L]ike the existing WORM requirement, [the audit-trail requirement] sets forth a specific and testable outcome that the electronic recordkeeping system must achieve: the ability to access and produce modified or deleted records in their original form.*[7] [emphasis added]

For clarity, the record and audit-trail requirement applies only to the final records required by regulation.

> *[T]he audit-trail requirement applies to the final records required pursuant to the rules, rather than to drafts or iterations of records that would not otherwise be required to be maintained and preserved under Rules 17a-3 and 17a-4 or Rules 18a-5 and 18a-6.*[8] [emphasis added]

2.1.2 Compliance Assessment

In this report, Cohasset has not assessed Google Cloud Storage in comparison to this requirement of the SEC Rules.

For enhanced control, a business-purpose recordkeeping system may store records and complete time-stamped audit-trails on Google Cloud Storage, with the features and controls described in Sections 2.2 through 2.9 of this report.

Reminder: This requirement is an alternative to the non-rewriteable, non-erasable record format requirement (i.e., write-once, read-many or WORM requirement), which is assessed in Section 2.2.

2.2 Non-Rewriteable, Non-Erasable Record Format

SEC 17a-4(f)(2)(i)(B) and 18a-6(e)(2)(i)(B):
Preserve the records exclusively in a non-rewriteable, non-erasable format

2.2.1 Compliance Requirement

This regulatory requirement was first adopted in 1997. In the 2022 Rule amendments, regulated entities are allowed to use a combination of electronic recordkeeping systems, to comply with each system meeting either (a) the non-rewriteable, non-erasable record format requirement described in this section or (b) the complete time-stamped record audit-trail requirement described in Section 2.1, *Record and Audit-Trail*.

The SEC further clarifies that the previously issued interpretations are extant. Therefore, records must be preserved in a non-rewriteable, non-erasable format that prevents overwriting, erasing, or otherwise altering records during the required retention period, which may be accomplished by any combination of hardware and software integrated controls.

> *The 2003 interpretation clarified that the WORM requirement does not mandate the use of optical disks and, therefore, a broker-dealer can use "an electronic storage system that prevents the overwriting, erasing or otherwise altering of a record during its required retention period through the use of integrated hardware and software [control] codes." The 2019 interpretation further refined the 2003 interpretation. In particular, it noted that the 2003 interpretation described*

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

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

> *a process of integrated software and hardware codes and clarified that "a software solution that prevents the overwriting, erasing, or otherwise altering of a record during its required retention period would meet the requirements of the rule."*
> *****
> *In 2001, the Commission issued guidance that Rule 17a-4(f) was consistent with the ESIGN Act. The final amendments to Rule 17a-4(f) do not alter the rule in a way that would change this guidance.*[9] [emphasis added]

Moreover, records must be preserved beyond established retention periods when certain circumstances occur, such as a subpoena or legal hold:

> *[A] broker-dealer must take appropriate steps to ensure that records are not deleted during periods when the regulatory retention period has lapsed but other legal requirements mandate that the records continue to be maintained, and the broker-dealer's storage system must allow records to be retained beyond the retentions periods specified in Commission rules.*[10] [emphasis added]

2.2.2 Compliance Assessment

It is Cohasset's opinion that the functionality of Google Cloud Storage, with the *Retention* features in *locked* mode, meets this SEC requirement to retain records in non-rewriteable, non-erasable format for the applied time-based[11] and event-based[12] retention periods and legal holds, when (a) properly configured, as described in Section 2.2.3 and (b) the considerations described in Section 2.2.4 are satisfied.

Reminder: This requirement is an alternative to the complete time-stamped audit-trail requirement, which is addressed in Section 2.1.

2.2.3 Google Cloud Storage Capabilities

This section describes the functionality of Google Cloud Storage that directly pertains to this SEC requirement to preserve electronic books and records in a non-rewriteable, non-erasable format, for the required retention period and any applied legal holds.

2.2.3.1 Overview

- Buckets, in Google Cloud Storage, are used to store records and their associated attributes.
- The *Retention* features must be properly configured for each Bucket that is intended to preserve records in compliance with SEC Rules, by applying one or more of the following options:
  - **Bucket Lock**: Retention attributes, including a *retention duration* and *locked* retention mode, are set for the Bucket and used to govern the immutable retention of all records stored in the Bucket. The Bucket's

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

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

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

12 Event-based retention periods require records to be retained indefinitely until a specified condition is met (e.g., a contract expires or an employee terminates), after which the record is retained for a fixed final retention period.

retention duration is used to dynamically calculate a *Retention Expiration Time* when determining deletion eligibility for stored records.

- **Object Retention Lock:** A pair of explicit retention controls (*Retain Until Time* and *locked* retention mode) are applied to the record at either (a) the time of initial recording or (b) anytime thereafter, for existing records. The explicit retention controls are stored as attributes of the record.
- **Bucket Lock and Object Retention Lock:** For Buckets configured to support both Bucket Lock and Object Retention Lock, stored records are retained for the longer of (a) the *Retention Expiration Time* that is dynamically calculated using Bucket Lock attributes and (b) the *Retain Until Time* that is explicitly stored with records as part of Object Retention Lock.

- Google Cloud Storage supports two types of indefinite holds that may be applied to records. Both types of holds are evaluated, in addition to Bucket Lock and Object Retention Lock, to determine deletion eligibility for a record.
  - The record's *Event Hold* attribute may be set (*True*) to indefinitely retain the record until set to *False*. The *Event Hold* attribute is designed to effectuate event-based, immutable retention; therefore, when the record's *Event Hold* attribute is changed from *True* to *False*, an *Event Hold Release Time* is automatically assigned and subsequently used when determining deletion eligibility. See subsection 2.2.3.3.3, *Applying Event Holds*, for details on this feature.
  - The record's *Temporary Hold* attribute may be set (*True*) to indefinitely retain the record until set to *False*. The *Temporary Hold* attribute is designed to immutably preserve records for litigation, regulatory investigation or other special circumstances. See subsection 2.2.3.4, *Temporary Holds (Legal Holds)*, for details on this feature.
- Optionally, versioning may be enabled for a Bucket that is configured for use with Object Retention Lock. When versioning is enabled, overwrites are allowed and result in a new version of the record with its own retention controls. *Note: Throughout this report, the term* ***record*** *refers to each* ***record version****, when versioning is enabled.*
- The following table summarizes the highly-restrictive integrated controls that are applied when the *Retention* features are utilized in *locked* mode. See the subsections following this *Overview*, for information on how to configure and apply the *Retention* and *Hold* features and details on the resulting integrated controls.

	***Retention* features in *locked* mode – highly-restrictive integrated retention controls**
Protecting record content and immutable attributes	• Immutability of the record content and key system attributes is enforced throughout the lifespan of the record: ○ When versioning is enabled, overwrites are allowed and result in new versions; each version is separately managed with its own retention controls. ○ When versioning is disabled, each record has only one version and overwrite attempts are prohibited, unless the existing record is eligible for deletion. • The record name and Bucket name cannot be changed.
Restricting changes to retention controls	• *Locked* retention mode, when configured for a Bucket (Bucket Lock) or explicitly applied to a record (Object Retention Lock), cannot be downgraded to *unlocked* or removed. • When in *locked* mode, retention periods (i.e., the *retention duration* for Bucket Lock and the *Retain Until Time* for Object Retention Lock) cannot be shortened or removed, though the retention period may be extended.

	***Retention* features in *locked* mode – highly-restrictive integrated retention controls**
Applying and removing indefinite holds	● When either the *Event Hold* or the *Temporary Hold* attribute is set (*True*) for a record, deletion eligibility is halted, and when set to *False*, the hold attribute no longer mandates indefinite, immutable retention. ○ A *Temporary Hold* attribute may be set (*True*) or removed (*False*) for records with or without other applied retention controls. ○ An *Event Hold* attribute may only be set (True) if the record's Object Retention Lock attributes were not previously set. ○ Additionally, when the *Event Hold* attribute is changed from *True* to *False* for a record, the *Event Hold Release Time* is automatically updated to current time to effectuate event-based retention.
Restricting deletion of Buckets and records	● Deletion is prohibited until the record is (a) past its dynamically calculated *Retention Expiration Time* and its explicitly applied *Retain Until Time* and (b) any holds (*Event Holds* and *Temporary Holds*) are removed (set to *False*). ● The Bucket cannot be deleted, unless it is empty, as long as the associated Account layer services (i.e., Projects) in Google Cloud are not removed. Additionally, a *Lien* may be set to prohibit Project deletion.

2.2.3.2 Bucket Configurations and Organizational Policies

- Google Cloud Storage Buckets are containers used to store records.
  - A Bucket name must be unique across the entire Google Cloud Storage namespace and cannot be changed after the Bucket is created.
  - The *Retention* features must be configured for each Bucket that is intended to retain records in compliance with the SEC Rules.
- The following table describes the options available when configuring a Bucket for use with the *Retention* features including (a) configuring Bucket Lock (left column), (b) enabling Object Retention Lock (right column), (c) setting a default *Event Hold* attribute and (d) creating supplementary Organizational Policies.

	Bucket Lock Configuration	**Object Retention Lock Configuration**
Configuring the *Retention* features	The Bucket Lock configuration applies retention controls to all records stored in the Bucket based on the following Bucket configurations. ● **Retention Duration**: A fixed *retention duration* is set as an attribute of the Bucket and is used to dynamically calculate the minimum time period that records are retained in the Bucket. ● **Retention Mode**: The retention mode must be set to ***locked***, a highly-restrictive mode, which ensures that the Bucket's fixed *retention duration* cannot be shortened, though it may be extended. Additionally, the *Retention* features in *locked* mode cannot be removed from the Bucket. ● Versioning must be disabled for a Bucket that is configured with Bucket Lock. ● The **Effective Date** for Bucket Lock is automatically set by Google Cloud Storage to the oldest record creation timestamp of the records being retained in that Bucket.	Object Retention Lock, when configured for a Bucket, enables explicit retention attributes (*Retain Until Time* and retention mode) to be applied to the record at either (a) the time of initial recording or (b) anytime thereafter, for existing records. ● Object Retention Lock must be enabled during initial Bucket creation, by setting the ***ObjectRetention*** attribute for the Bucket to *True*. ● Once Object Retention Lock is enabled for a Bucket it cannot be disabled. Optionally, **versioning** may be enabled for a Bucket that is configured for use with Object Retention Lock. ● When versioning is enabled, overwrites are allowed, which results in a new version of the record with its own, separate retention and hold controls. ● If versioning is disabled, each record has only one version and overwrites are disallowed, unless the existing record is eligible for deletion.

	Bucket Lock Configuration	Object Retention Lock Configuration
	○ When Bucket Lock is first configured, the effective date is the current timestamp. Thereafter, if the Bucket's fixed *retention duration* is extended, the effective date is the most recent of: ▪ The prior effective date, if none of the previously written records have expired, or ▪ The *retention duration* change timestamp minus the full duration of the *prior* Bucket *retention duration*.	● If versioning is suspended (i.e., changed from enabled to disabled) existing record versions stored in the Bucket are unaffected, but the Bucket no longer allows the storage of new noncurrent versions.
Configuring a combination of Bucket Lock and Object Retention Lock	Both Bucket Lock and Object Retention Lock can be configured on a single Bucket. ● When both Bucket Lock and Object Retention Lock are configured, the Bucket *retention duration* ensures that all records stored in the Bucket are kept for at least as long as the Bucket *retention duration* and a record's *Retain Until Time* is honored when it requires longer retention. ● Versioning is supported for use with Object Retention Lock only. Therefore, Buckets that are configured for use with both Bucket Lock and Object Retention Lock must have versioning disabled.	
Setting *Event Hold* as Bucket default	When the default *Event Hold* attribute is enabled (*True*) for a Bucket, **new** records inherit the *Event Hold* (*True*) value, which is stored as an attribute of the record. Additionally, each record's specific *Event Hold* attribute may be changed at any time. ● The Bucket's default *Event Hold* feature is independent of Bucket Lock and Object Retention Lock configurations. However, the *Event Hold* attribute may be set (*True*) only if the record's Object Retention Lock attributes are not set. ● See subsection 2.2.3.3.3, *Applying Event Holds*, for details on this feature.	
Setting Organizational Policies	When relying on Bucket Lock, Cohasset encourages the regulated entity to set the following Organizational Policies at the organization, folder, or project level, which are then inherited down through the hierarchy, to supplement compliance with the SEC Rule. ● Require Buckets to be configured with Bucket Lock. ● Require Bucket Lock configurations to match a configured option. Note: Organization Policies are not applied retroactively and are only 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 set-up, or retention policies for existing Buckets must be manually updated, as needed.	Not Applicable.
Setting Project *Liens*	Cohasset encourages the regulated entity to setup a *Lien* on Projects that contain Buckets configured with *Retention* features. A *Lien* prevents Bucket deletion, even by an administrator, until the *Lien* is removed. This is useful in preventing accidental Bucket deletion.	

2.2.3.3 Record Definition and Retention Controls

- Each record stored in Google Cloud Storage is comprised of:
  - Complete content of the record.
  - Immutable record attributes, e.g., record name, generation number (version identifier), creation (storage) timestamp, size, and object checksums.

- The record name (or record name and generation number, if versioning is enabled) must be unique within the Bucket where it is stored.

- Mutable record attributes, e.g., *Event Hold* attribute, *Temporary Hold* attribute, user-specified custom attribute tags.
  - When Object Retention Lock is applied in *locked* mode, the record's explicitly stored *Retain Until Time* may be extended, but not shortened or removed.
  - The *Event Hold* attribute may be set (*True*) only if the record's Object Retention Lock attributes are not set.

2.2.3.3.1 Applying Bucket Lock

- Bucket Lock applies a *retention duration* to all records stored in the Bucket. When the Bucket Lock mode is *locked*, the *retention duration* cannot be shortened or removed by any user, which assures that a minimum retention period automatically applies to all records stored in the Bucket.
- When using Bucket Lock for time-based retention, which requires the record to be retained for a specified period of time from the record creation timestamp:
  - A *Retention Expiration Time* is dynamically calculated for each record by adding the Bucket's current *retention duration* to the record's creation timestamp. This calculation occurs during operations, such as determining if a record is eligible for deletion or overwrite and during GET operations (i.e., requesting data).
  - The record content, together with its immutable attributes, are protected from being deleted, until the calculated *Retention Expiration Time* is in the past. (See Section 2.2.3.5, *Deletion Controls*, for additional information on determining deletion eligibility.)
- If the Bucket *retention duration* is *extended*, the longer duration automatically (a) applies retroactively to records currently stored in the Bucket and (b) applies to new records added to the Bucket.
- Additionally, when a record's *Event Hold* has been changed from *True* to *False*, the record's *Event Hold Release Time* is set and the *Retention Expiration Time* is dynamically calculated by adding the Bucket's current *retention duration* to the record's *Event Hold Release Time*. See subsections 2.2.3.3.3, *Applying Event Holds,* and 2.2.3.5, *Deletion Controls*, for additional information.

2.2.3.3.2 Applying Object Retention Lock

- For compliance with the Rules using Object Retention Lock, two retention attributes must be explicitly stored for each record: (1) retention mode of *locked* and (2) a *Retain Until Time* that meets regulatory requirements.
  - When the retention mode is set to *locked* for a record, the retention mode cannot be changed or removed and the *Retain Until Time* can only be extended (not shortened or removed). Therefore, the record is immutably retained until eligible for deletion. (See Section 2.2.3.5, *Deletion Controls*, for additional information on determining deletion eligibility.)
- These two retention controls (*locked* retention mode and *Retain Until Time*) must be set as a pair for each record that is a required record for compliance with the Rules.

- The attributes may be transmitted with the record, when it is being stored, or may be set at a later time.
- If only one attribute is transmitted the operation will fail.
- If the *Event Hold* attribute is set (*True*) for the record, operations to apply Object Retention Lock attributes will fail.

- When versioning is *enabled,* overwrites of a record are allowed, which result in a new version with its own separately stored retention mode and *Retain Until Time*. If a specific record version is not specified, retention controls are applied to the live (top) version only. When versioning is *disabled*, overwrites are prohibited.

2.2.3.3.3 Applying *Event Holds*

- For records that require event-based retention, (i.e., retained for an indefinite period of time until an *event* occurs, such as the closure of a customer account or termination of a contract, and thereafter, for a fixed duration of time):
  - The *Event Hold* attribute for the record is set to *True*, either by (a) inheriting the Bucket's *default* value or (b) having it explicitly set. When set to *True,* it enforces immutability and prohibits deleting or changing the record.
  - When the *Event Hold* attribute is changed from *True* to *False* for a specific record, the current time is stored as the record's *Event Hold Release Time,* and immutable retention and deletion eligibility are controlled by the applied *Retention* features as follows:
    - **Bucket Lock**: The *Retention Expiration Time* is dynamically calculated by adding the current Bucket *retention duration* to the record's *Event Hold Release Time*. This calculation occurs during operations such as determining if a record is eligible for deletion or overwrite, and during GET operations. The record is protected as immutable and cannot be deleted until the calculated *Retention Expiration Time* is in the past. (See Section 2.2.3.5, *Deletion Controls*, for additional information on determining deletion eligibility.)
    - **Object Retention Lock**: When a record's *Event Hold* is *False*, its retention mode and *Retain Until Time* attributes may be set.
      - If only Object Retention Lock controls apply to the record, the *locked* retention mode and *Retain Until Time* attributes must be set immediately upon changing the *Event Hold* to *False*, **to assure continued immutable retention.**
      - Note: Object Retention Lock attributes may only be applied to a record if the record's *Event Hold* attribute is *False*. Conversely, if a record's Object Retention Lock attributes were previously set, the *Event Hold* attribute may **not** be set to *True*. Furthermore, if both *Event Hold* and Object Retention Lock attributes are attempted to be set during the write process, the write process fails and an error will result.
    - **Both Bucket Lock and Object Retention Lock**: Also see Section 2.2.3.3.4 *Applying a Combination of Bucket Lock, Object Retention Lock, and Event Holds*.
- The record's *Event Hold Release Time* cannot be modified by any administrator or 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, 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 once again enforces immutability and prohibits deleting the record. The existing *Event Hold Release Time* remains unchanged, until it is populated with the current time when the *Event Hold* attribute is changed from *True* to *False*.
- If versioning is enabled and the record version is not specified when changes are made to the *Event Hold* attribute, the changes are applied to the live (top) version only.

2.2.3.3.4 Applying a Combination of Bucket Lock, Object Retention Lock, and *Event Holds*

- A Bucket may be configured to support both Bucket Lock and Object Retention Lock. Additionally, the *Event Hold* feature may be utilized to manage event-based retention. The following table describes the retention controls that are applied when these features are combined.
  - The column with the green heading explains that a Bucket *retention duration* is set for all rows, since this subsection pertains to the application of both Bucket Lock and Object Retention Lock. For compliance with SEC Rules, the retention mode for the Bucket is set to *locked*.
  - The columns with orange headings list the *Event Hold* and *Event Hold Release Time* values stored for a specific record.
    - The record's *Event Hold* attribute is either set by the Bucket default or is transmitted for the record.
    - The *Event Hold Release Time* is automatically set to the current time and stored as an attribute of the record when the *Event Hold* attribute changes from *True* to *False*.
  - The columns with gold headings list the retention mode and *Retain Until Time* attributes set for a specific record.
  - The column with a blue heading explains the retention applied to the specific record.

	***Bucket Lock* configuration**	**Record-level *Event Hold* attribute values**		**Record-level *Object Retention Lock* attribute values**		
	Bucket *retention duration*	***Event Hold***	***Event Hold Release Time***	***Retention Mode***	***Retain Until Time***	**Retention applied for the record**
1.	Bucket *Retention Duration*	*False*	Null	Null	Null	• The record's *Retention Expiration Time* is dynamically calculated by adding the Bucket *retention duration* to the record's creation timestamp.
2.	Bucket *Retention Duration*	*True*	Null	Null	Null	• The record is immutably retained until the *Event Hold* attribute is changed to *False*. (See next row).
3.	Bucket *Retention Duration*	*False*	mm/dd/yyyy	Null	Null	• When the record's *Event Hold* attribute is changed from *True* to *False*, the current time is automatically stored as the record's *Event Hold Release Time*. • The record's *Retention Expiration Time* is dynamically calculated by adding the Bucket *retention duration* to the record's *Event Hold Release Time*.

	***Bucket Lock* configuration**	**Record-level *Event Hold* attribute values**		**Record-level *Object Retention Lock* attribute values**		
4.	Bucket *Retention Duration*	*False*	Null	Locked	mm/dd/yyyy	• The record is retained for the longer of: ○ The *Retain Until Time* (mm/dd/yyyy) ○ The sum of the *Bucket retention duration* added to the record's creation timestamp.
5.	Bucket *Retention Duration*	*True*	Null	Locked	mm/dd/yyyy	• Disallowed; error will result.
6.	Bucket *Retention Duration*	*False*	mm/dd/yyyy	Locked	mm/dd/yyyy	• The record is retained for the longer of: ○ The *Retain Until Time* (mm/dd/yyyy) ○ The sum of the *Bucket retention duration* added to the record's *Event Hold Release Time*. • Note: This occurs when the record's Object Retention Lock attributes are set after the record's *Event Hold* attribute is changed from *True* to *False*, which sets the record's *Event Hold Release Time*.

2.2.3.3.5 Record Operations and Retention Controls

- The following table describes the integrated controls applied by the *Retention* features, in *locked* mode. The described controls apply whether Bucket Lock, Object Retention Lock, or both types of *Retention* apply to the record, unless otherwise explained.

	The *Retention* Features in the Highly-restrictive *Locked* Mode.
Uniquely identifying records and protecting immutable attributes	• The Global Identifier for each record, is comprised of (a) the Bucket name, which is unique across the entire Google Cloud Storage namespace, (b) a record name, which is unique within the Bucket, unless versioning is enabled, and (c) an automatically assigned generation number (version identifier). • Each of these attributes is immutable.
Managing versions and protecting record content	• Optionally, versioning may be enabled for a Bucket that is configured for use with Object Retention Lock. • When versioning is enabled: ○ Each *version of an object* is separately managed for retention, i.e., Object Retention Lock controls separately apply to each version. ○ Attempts to overwrite an existing record results in storing a new record version with a unique generation number and applied retention controls. Each record version is immutably stored for its lifespan. • When versioning is *disabled:* ○ Each record has only one version and its record contents are immutably stored for its lifespan. ○ Attempts to overwrite an existing record that is eligible for deletion, results in deleting the existing eligible record and replacing it with a new record with a unique generation number. ○ Attempts to overwrite an existing record that is not eligible for deletion, results in reporting an error message through the Google Cloud Console, and the new record is not stored. • When versioning is suspended (i.e., changed from enabled to disabled): ○ Existing record versions stored in the Bucket are unaffected, but the Bucket no longer allows the storage of new noncurrent versions.

	The *Retention* Features in the Highly-restrictive *Locked* Mode.
Modifying or removing retention controls	● For Bucket Lock in *locked* mode: ○ The Bucket *retention duration* cannot be shortened or removed; only extended as necessary. If the Bucket *retention duration* is *extended*, the longer duration automatically (a) applies retroactively to records currently stored in the Bucket and (b) applies to new records added to the Bucket. ○ The Bucket's retention mode cannot be changed from *locked* to *unlocked* and cannot be removed. ● For Object Retention Lock: ○ If a record is set to *locked* retention mode, the retention mode cannot be changed to *unlocked* and cannot be removed, and the *Retain Until Time* can only be extended (not shortened or removed). ○ If the record version is not specified, changes made to the retention mode and *Retain Until Time* are applied to the live (top) version only. ○ If only one retention attribute is specified, the update is rejected; retention mode and the *Retain Until Time* must be set as a pair.
Modifying *Event Hold* attribute	● A record's *Event Hold* attribute may be set to *True*, unless the record's retention mode and *Retain Until Time* attributes were previously set. ● A record's *Event Hold* attribute may be set to *False* at any time.
Modifying Legal Hold attribute	● A record's *Temporary Hold* (Legal Hold) attribute may be set to *True* or *False*, whether or not retention controls are applied to the Bucket or to the specific record. See Section *2.2.3.4 Temporary Holds (Legal Holds)* for additional information.
Restricting deletion	● Deletion attempts by any user or process are rejected unless all applied retention controls are expired and *Hold* attributes (*Event Hold* and *Temporary Hold*) are *False*. ○ When versioning is enabled, the generation number must be specified when deleting a record. If the generation number is not specified, Google Cloud Storage retains the record as a noncurrent version, rather than 'deleting' the live (top) version. ● See Section 2.3.3.5, *Deletion Controls*, for additional information.
Copying records	● A record may be *copied* between Buckets, resulting in the creation of a new copy with its own unique attributes, including the assignment of a new creation timestamp, based on the time the copy was stored. ● Separate retention controls and the *Hold* attributes apply to the new copy, in accordance with the configurations of the target Bucket and the retention attributes set on the copy.
Moving records	● A record under active retention cannot be *moved* between Buckets.
Tiering storage classes	● Retention controls apply across all storage classes. Therefore, a record under *locked* retention may be *moved* to a different storage class. All applied retention controls remain with the record.
Changing permissions	● Read permissions for a record may be changed (expanded or contracted) at any time.

2.2.3.4 Temporary Holds (Legal Holds)

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

- The *Temporary Hold* is a simple *True/False* Boolean value for each stored record.
  - When the *Temporary Hold* flag is *True,* it enforces immutability and prohibits both overwrite and deletion of the record until the hold is removed (set to *False*).

- If versioning is enabled and the record version is not specified when setting a *Temporary Hold*, the *Temporary Hold* is applied to the live (top) version only.
- *Temporary Hold*s may be placed on records that are under an *Event Hold*.

- When the *Temporary Hold* is *False,* this attribute no longer mandates preservation of the record; however *other controls* may continue to protect the record.

- Optionally, the reason for applying the hold may be stored in custom attributes, though this is not required.

2.2.3.5 Deletion Controls

- The record, together with its attributes, is *eligible for deletion* when **all** of the following conditions (if applicable) are met:
  - The Bucket's *retention duration* value added to the record's creation timestamp is in the past.
  - The Bucket's *retention duration* value added to the record's *Event Hold Release Time* is in the past.
  - The record's stored *Retain Until Time* is in the past.
  - The record's *Event Hold* attribute is *False*.
  - The record's *Temporary Hold* (Legal Hold) attribute is *False*.
- When versioning is enabled and the generation number is not specified as part of a delete request, Google Cloud Storage retains it as a noncurrent object version, rather than 'deleting' the live (top) version.
- Deletion may be initiated by:
  - API (Application Programming Interface), UI (User Interface) or CLI (Command Line Interface), when the user has appropriate authorizations.
  - Object Lifecycle Management actions configured to delete records.

  Note: Deletion actions are successful only for records that are *eligible for deletion*.
- A *Lien* may be configured to prohibit the deletion of an Account Layer Project, thereby preventing deletion of associated Buckets.

2.2.3.6 Security

- Google Cloud Storage supports setting permissions and access controls for each Bucket, via Identity and Access Management tools.
- SSL (Secure Socket Layer) policies may be configured to specify a minimum TLS (Transport Layer Security) version and a profile that selects a set of SSL features to enable. The profiles are available; the first three are managed by Google:
  1. **Compatible**: Allows the broadest set of source systems to negotiate SSL.
  2. **Modern**: Supports a wide set of SSL features, allowing modern source systems to negotiate SSL.
  3. **Restricted**: Supports a reduced set of SSL features, intended to meet stricter compliance requirements.

4. **Custom**: Allows the administrator to select SSL features individually.

- Records and attributes are encrypted:
  - Google Cloud Storage currently performs all operations using transport-layer encryption (HTTPS) to protect against data leakage over shared networks.
  - Google Cloud Storage encrypts data at rest and automatically decrypts the data, to render it for use.
    - Google Cloud Storage offers the Google Cloud Key Management System (KMS) to protect data at rest.
    - The regulated entity may elect to use their own external third-party KMS if desired.
  - The regulated entity may encrypt records prior to uploading to Google Cloud Storage. The regulated entity is responsible for maintaining its encryption keys.
- Independent third-party audits of Google's infrastructure, services and operations are undertaken on a regular basis to verify security, privacy and compliance controls.

2.2.3.7 Clock Management

Google Cloud Storage 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 attributes are fully written.

2.2.4 Additional Considerations

In addition, for this requirement, the regulated entity is responsible for:

- Enabling versioning if overwrite capability is required. When versioning is enabled, appropriate retention controls and *Hold* attributes (Event and Temporary) must be separately applied and managed for each version.
- Configuring each Bucket intended to store records in compliance with SEC Rules with the *Retention* features (i.e., Bucket Lock, Object Retention Lock, or both), when the Bucket is first created.
- Setting the retention mode to ***locked***, when using Bucket Lock, which applies highly-restrictive, integrated control codes that extend to the storage subsystem and systemically disallow administrators from shortening or removing retention controls.
- Setting the fixed *retention duration* associated with Bucket Lock to the longest retention period for all records to be stored in the Bucket.
- Transmitting an appropriate *Retain Until Time* and a ***locked*** retention mode with each record, when using Object Retention Lock.
- Setting the *Event Hold* to *True* to retain records indefinitely while a specific condition exists, such as *while the customer account is open*, and setting the *Event Hold* to *False* when the condition/event has been met. If using

Object Retention Lock only, ensuring a *locked* retention mode and appropriate *Retain Until Time* are immediately applied to records when the *Event Hold* is set to *False*.

- Applying a *Temporary Hold* to records that require preservation for legal matters, government investigations, external audits and other similar circumstances, and releasing the *Temporary Hold* when the applicable action is completed.
- Ensuring all records required to be retained for compliance with the SEC Rule are protected with appropriate retention controls within 24 hours of creation or are stored in an SEC-compliant protected storage system until they are uploaded to Google Cloud Storage.

Additionally, the regulated entity is responsible for (a) maintaining its Google Cloud *Account layer* (Organization, Folder and Project) in good standing and paying for appropriate technology and services to allow records to be retained until the applied retention periods and holds have expired or until the records have been transferred to another compliant storage system, (b) authorizing user privileges, and (c) maintaining appropriate resources, encryption keys, and other information and services needed to retain the records. Similar to decommissioning a datacenter, deleting a Project in the Account layer will delete Buckets and records, even if the records are not eligible for deletion. As a safeguard:

- Set a *Lien* to prohibit the deletion of an Account Layer Project, thereby protecting associated Buckets and their records from being prematurely deleted.
- Assign the authority to create Projects to a compliance administrator role and then delegate responsibility of day-to-day management to a separate IT system administrator, without the permission to delete the project. This prevents the IT system administrator from removing the *Lien* and deleting the associated Buckets.

2.3 Record Storage Verification

2.3.1 Compliance Requirement

SEC 17a-4(f)(2)(ii) and 18a-6(e)(2)(ii):
Verify automatically the completeness and accuracy of the processes for storing and retaining records electronically

The electronic recordkeeping system must automatically verify the completeness and accuracy of the processes for storing and retaining records electronically, to ensure that records read from the system are precisely the same as those that were captured.

This requirement includes both quality verification of the recording processes for storing records and post-recording verification processes for retaining complete and accurate records.

2.3.2 Compliance Assessment

Cohasset affirms that the functionality of Google Cloud Storage meets this SEC requirement for complete and accurate recording of records and post-recording verification processes, when the considerations identified in Section 2.3.4 are satisfied.

2.3.3 Google Cloud Storage Capabilities

The recording and post-recording verification processes of Google Cloud Storage are described below.

2.3.3.1 Recording Process

- Google Cloud Storage records an immutable checksum of the data written for any record and verifies the checksum on subsequent operations on the record. See *Post-Recording Verification Process*, below.
- When uploading a record, the source system may submit a checksum. When a checksum is provided, the record will only be stored if the checksum calculated by Google Cloud Storage for the record matches the user-provided checksum. If it does not match, an error is reported to the user audit event log and the object must be re-uploaded.
- When a record is uploaded to Google Cloud Storage, a *success* response is sent to the source system. This also indicates that the record has been replicated.
- Google Cloud Storage maintains integrity information at each component of the internal architecture.

2.3.3.2 Post-Recording Verification Process

- Regular data integrity checks are performed in the background by reading all data written and validating the corresponding checksums. Inbuilt validation of checksums for correctness, integrity and durability are processed frequently (at least every two weeks), eliminating the need for manual health check processes.
- If an invalid checksum is found, the data is immediately corrected, typically without having to go to additional sources for the data (since all copies are stored with high durability).
- Google Cloud Storage durability features validate the record content and are designed to assure 11-nines of durability for all storage classes.
- When a record is retrieved, if any part of the data is incorrect, the Google Cloud Storage durability features automatically recover or regenerate an accurate replica.

2.3.4 Additional Considerations

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

2.4 Capacity to Download and Transfer Records and Location Information

2.4.1 Compliance Requirement

SEC 17a-4(f)(2)(iv) and 18a-6(e)(2)(iv):
Have the capacity to readily download and transfer copies of a record and its audit-trail (if applicable) in both a human readable format and in a reasonably usable electronic format and to readily download and transfer the information needed to locate the electronic record, as required by the staffs of the Commission, [and other pertinent regulators] having jurisdiction over the [regulated entity]

This requirement calls for an adequate capacity to readily download records and information needed to locate the record in both a:

- Human readable format that can be naturally read by an individual, and
- Reasonably usable electronic format that is compatible with commonly used systems for accessing and reading electronic records.

The downloaded records and information needed to locate the records (e.g., unique identifier, index, or properties) must be transferred to the regulator, in an acceptable format.

Further, this requirement to download and transfer the complete time-stamped audit-trail applies only when this alternative is utilized; see Section 2.1, *Record and Audit-Trail*.

2.4.2 Compliance Assessment

It is Cohasset's opinion that the functionality of Google Cloud Storage meets this SEC requirement to maintain the capacity to readily download and transfer the records and information used to locate the records, when the considerations described in Section 2.4.4 are satisfied.

2.4.3 Google Cloud Storage Capabilities

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

- Each record is uniquely identified by the Global Identifier, which is comprised of (a) the Bucket name, which is unique across the entire Google Cloud Storage namespace, (b) a record name, which is unique within the Bucket, and (c) generation number. Each of these attributes is immutable and retained for the same duration as the record.
- The creation timestamp captured and stored with each record in a Bucket is immutable and retained for the same duration as the record.
- Google Cloud Storage assures that their hardware and software capacity allows for ready access to the records and attributes. Further, Google Cloud Storage 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.
- Authorized users can (a) list or search the Bucket name, (b) list records in lexicographic order, (c) search the record name, and (d) download the record and a text file containing the associated attributes to a designated storage location. Record attributes, include:
  - Immutable Bucket attributes, e.g., Bucket name, creation timestamp.

- Mutable Bucket attributes, e.g., Bucket labels and the Bucket *retention duration*.
- Immutable record attributes, e.g., record name, generation number, creation timestamp, *locked* retention mode, size, and record checksums.
- Mutable record attributes, e.g., *Event Hold, Event Hold Release Time, Temporary Hold, Retain Until Time* (for Object Retention Lock), and user-specified attribute tags for records.

▶ Records and associated attributes may be downloaded by authorized users.

2.4.4 Additional Considerations

The regulated entity is responsible for (a) maintaining its account in good standing, (b) authorizing user privileges, (c) maintaining appropriate technology and resource capacity, encryption keys, and other information and services needed to use Google Cloud Storage to readily access, download, and transfer the records and the information needed to locate the records, and (d) providing requested information to the regulator, in the requested format.

2.5 Record Redundancy

2.5.1 Compliance Requirement

The intent of this requirement is to retain a persistent alternate source to reestablish an accessible, complete and accurate record, should the original electronic recordkeeping system be temporarily or permanently inaccessible.

The 2022 final Rule amendments promulgate two redundancy options, paragraphs (A) or (B).

SEC 17a-4(f)(2)(v) and 18a-6(e)(2)(v):

(A) Include a backup electronic recordkeeping system that meets the other requirements of this paragraph [(f) or (e)] and that retains the records required to be maintained and preserved pursuant to [§ 240.17a-3 or § 240.18a-5] and in accordance with this section in a manner that will serve as a redundant set of records if the original electronic recordkeeping system is temporarily or permanently inaccessible; or

(B) Have other redundancy capabilities that are designed to ensure access to the records required to be maintained and preserved pursuant to [§ 240.17a-3 or § 240.18a-5] and this section

▶ The intent of paragraph (A) is:

[B]ackup electronic recordkeeping system must serve as a redundant set of records if the original electronic recordkeeping system is temporarily or permanently inaccessible because, for example, it is impacted by a natural disaster or a power outage.[13] [emphasis added]

▶ The intent of paragraph (B) is:

[R]edundancy capabilities that are designed to ensure access to Broker-Dealer Regulatory Records or the SBS Entity Regulatory Records must have a level of redundancy that is at least equal to the level that is achieved through using a backup recordkeeping system.[14] [emphasis added]

Note: The alternate source, must meet *"the other requirements of this paragraph [(f)(2) or (e)(2)]"*, thereby disallowing non-persistent copies that are overwritten on a periodic basis, resulting in a much shorter retention period than the original.

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

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

2.5.2 Compliance Assessment

Cohasset upholds that the functionality of Google Cloud Storage meets both paragraphs (A) and (B) of this SEC requirement by retaining a persistent redundant copy of the records or alternate source to reestablish the records, when (a) properly configured as described in Section 2.5.3 and (b) the considerations described in Section 2.5.4 are satisfied.

2.5.3 Google Cloud Storage Capabilities

The two options for meeting the record redundancy requirement are described in the following subsections.

2.5.3.1 Redundant Set of Records

- For compliance with paragraph (A), to maintain a redundant set of records, each Bucket is configured with a storage location type which determines the replication services available for records added to the Bucket.
  - Records added to the Bucket use the configured storage location type unless specified otherwise.
  - Any changes to the storage location type applies to records that are added day forward and will not apply retrospectively to records that are already in the Bucket.
  - Further, the API may (a) specify the storage location type of individual records being added to a Bucket or (b) change the storage location type for a record.
- Storage location types include:
  - **Multi-Regional or Dual-Region location types** provide asynchronous geo-redundancy 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 are retained.
  - **Regional location type** provides redundancy across multiple availability zones within the designated region, in addition to redundancy across multiple disks, power, and network failure domains.
- Additionally, each Bucket can be configured with a storage class during the Bucket creation process. The storage class determines the availability of records (i.e., the expected latency and monthly uptime). Options range from Standard storage, which offers the best performance and availability for frequently accessed data, to Nearline, Coldline and Archive storage options for less-frequently accessed data.
  - All storage classes are offered for each storage location type and do not affect the replication services described above.
- Optionally, Google Cloud Storage Object Lifecycle Management and Autoclass features may perform an *in-place* downgrade of an object's storage-class. These processes do **not** change the content or retention attributes stored for the record. Accordingly, these in-place downgrade requests do not conflict with the *Retention* features and are allowed for records under retention controls.
- Replicas of records are retained for the same time period as the original records.

2.5.3.2 Other Redundancy Capabilities

- For compliance with paragraph (B), all storage classes available to Google Cloud Storage are designed for 11-nines of 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 records can be accurately regenerated from the erasure coded data segments even in the event of the simultaneous loss of two disks.

2.5.4 Additional Considerations

In addition, for this requirement, the regulated entity is responsible for: (a) maintaining its account in good standing and (b) maintaining appropriate technology and resource capacity, encryption keys, and other information and services needed to use Google Cloud Storage and permit access to the redundant records.

2.6 Facilities to Produce Records for Examination

2.6.1 Compliance Requirement

SEC 17a-4(f)(3)(i) and 18a-6(e)(3)(i):
At all times have available, for examination by the staffs of the Commission, [and other pertinent regulators], facilities for immediately producing the records preserved by means of the electronic recordkeeping system and for producing copies of those records

The intent of this requirement is for the regulated entity to be ready at all times (with facilities and technology) to immediately and easily provide records stored on an electronic recordkeeping system to the regulator for examination. The records may be produced as a human-readable view, print or other reproduction method that allows the regulator immediate and easy access to the requested records.

The regulator may need to use the facilities to access the records, in rare instances, such as financial failure of the regulated entity or insufficient availability of staff to respond to regulator requests to produce records.

2.6.2 Compliance Assessment

Cohasset affirms that Google Cloud Storage supports the regulated entity's compliance with this SEC requirement to have sufficient facilities and technology available to immediately produce human-readable renderings of the records.

2.6.3 Google Cloud Storage Capabilities

The regulated entity is responsible for providing adequate facilities and technology to produce records for examination, and compliance is supported by Google Cloud Storage.

- As a cloud-based service, Google maintains adequate technology resources for Google Cloud and Google Cloud Storage to deliver its services to the regulated entity on demand over the internet, to local computers.
  - All the storage classes available to Google Cloud Storage are designed for 11-nines of durability.
  - At any given time, data availability on Google Cloud Storage ranges from 99.0% to 99.99%, based on the Storage class selected by the regulated entity.

- Records are automatically replicated, across multiple availability zones or geo-replicated across dual or multi-regional storage locations.
- The regulated entity, and optionally the regulator, may access Google Cloud and Google Cloud Storage, using local computers and internet services.

▶ Google Cloud Storage delivers records for a browser or other local tools to render human-readable images.

- Google Cloud Storage encrypts data at rest and automatically decrypts the data, when rendering the record for use.
  - Google Cloud Storage offers the Google Cloud Key Management System (KMS) to protect data at rest, or
  - the regulated entity may elect to use their own external third-party KMS if desired.
- Records may be viewed or printed from a browser or downloaded via Google Cloud Storage LIST and GET APIs for local facilities to render a human-readable projection or print of the records.

2.6.4 Additional Considerations

Cohasset recommends using HTTPS (a secure internet transfer protocol), when practical, to reduce the chance of network-level errors when transmitting and inputting the records.

In addition, for this requirement, the regulated entity is responsible for: (a) maintaining its account in good standing, (b) authorizing user privileges, (c) maintaining appropriate technology, facilities, and resource capacity, and encryption keys in order to use Google Cloud Storage to readily access, download, and transfer the records, and (d) providing requested records to the regulator, in the requested format.

2.7 Provide Records to Regulators

SEC 17a-4(f)(3)(ii) and 18a-6(e)(3)(ii):
Be ready at all times to provide, and immediately provide, any record stored by means of the electronic recordkeeping system that the staffs of the Commission, [and other pertinent regulators] having jurisdiction over the [regulated entity] may request

2.7.1 Compliance Requirement

This requires the regulated entity, using an electronic recordkeeping system, to immediately provide the regulator with requested records.

The records may be produced as a human-readable view, print or other reproduction method that allows the regulator immediate and easy access to the requested records.

2.7.2 Compliance Assessment

Cohasset upholds that Google Cloud Storage supports the regulated entity in meeting this SEC requirement to immediately provide regulators with reproductions of the records.

2.7.3 Google Cloud Storage Capabilities

The regulated entity is responsible for producing records for regulators, and compliance is supported by Google Cloud Storage.

- Google Cloud Storage uniquely identifies each record and provides search and download capabilities, which facilitates providing records to regulators; see Section 2.4, *Capacity to Download and Transfer Records and Location Information*.
- As a cloud-based service, Google maintains adequate technology resources for the regulated entity to readily access its stored records, using local computers and internet services, as described in Section 2.6 *Facilities to Produce Records for Examination*.

2.7.4 Additional Considerations

- The regulated entity is responsible for producing records for regulators in the requested format and medium.

2.8 Audit System

2.8.1 Compliance Requirement

For electronic recordkeeping systems that comply with the non-rewriteable, non-erasable format requirement, as stipulated in Section 2.2, *Non-Rewriteable, Non-Erasable Record Format*, the Rules require the regulated entity to maintain an audit system for accountability (e.g., when and what action was taken) for both (a) inputting each record and (b) tracking changes made to every original and duplicate record. Additionally, the regulated entity must ensure the audit system results are available for examination for the required retention time period stipulated for the record.

SEC 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii):

For a [regulated entity] operating pursuant to paragraph [(f)(2)(i)(B) or (e)(2)(i)(B)] of this section, the [regulated entity] must have in place an audit system providing for accountability regarding inputting of records required to be maintained and preserved pursuant to [§ 240.17a-3 or § 240.18a-5] and this section to the electronic recordkeeping system and inputting of any changes made to every original and duplicate record maintained and preserved thereby.

(A) At all times, a [regulated entity] must be able to have the results of such audit system available for examination by the staffs of the Commission [and other pertinent regulators].

(B) The audit results must be preserved for the time required for the audited records

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

2.8.2 Compliance Assessment

Cohasset asserts that Google Cloud Storage, in conjunction with detailed Cloud Audit Logs, when enabled as a Google Cloud service, supports the regulated entity's efforts to meet this SEC requirement for an audit system.

2.8.3 Google Cloud Storage Capabilities

The regulated entity is responsible for an audit system and the following Google Cloud Storage capabilities support the regulated entity in meeting this requirement.

- When inputting records, Google Cloud Storage stores a unique Global Identifier, system-generated creation (storage) timestamp and generation number for each record. These attributes are immutable, chronologically account for each inputted record and are retained for the same time period as the record.
  - The Global Identifier is comprised of (a) the Bucket name, which must be unique across the entire Google Cloud Storage namespace, (b) a record name, which must be unique within the Bucket where it is stored, and (c) generation number. Each of these attributes are immutable.

- If the record name is not unique, the record is not stored, and an error message is reported through the interface used to store the record (e.g., API, CLI) as well as the Google Cloud Console.

- In addition to the immutable Global Identifier and system-generated creation timestamp, Google Cloud Storage provides Cloud Audit Logging, which is a Google Cloud service that maintains Administrative Activity logs and Data Access logs and makes the logs available for a period of time through the Google Cloud Console. Note: The Cloud Audit Logging service must be set to *Detailed Audit Logging Mode* in order to capture events specific to the modification of *Retention* configurations.
  - Administrative Activity logs document operations that modify the configuration or attributes of a Project or Bucket. Examples of captured operations include:
    - Creating and deleting Buckets.
    - Configuring Buckets for use with the *Retention* features.
    - Setting and changing Identity and Access Management (IAM) policies.
    - Updating Bucket attributes.
  - 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.
- Authorized system administrators for the regulated entity can use the Google Cloud Audit Logging service to:
  - Search and filter audit events by:
    - *Audit Log Name:* Audit events are assigned to logs within projects and organizations.
    - *Resource:* Each audit entry tracks the associated Google Cloud resource.
    - *Service:* Services are individual products, such as Compute Engine, Cloud SQL, or Cloud Pub/Sub.
  - Export the selected audit events and retain the audit results for the required retention period. Options include:
    - Configuring the automatic export of log entries to a Google Cloud Storage Bucket, configured with the appropriate R*etention* features. Optionally, setting the retention mode to *locked*, which applies strict retention controls.
    - Importing log entries into the regulated entity's (non-Google Cloud) security information event management tool, and then use that tool and data to retain the audit events for the required retention period.
- Additionally, the effective date of the Bucket Lock controls is maintained as an attribute of the Bucket.

2.8.4 Additional Considerations

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

2.9 Information to Access and Locate Records

2.9.1 Compliance Requirement

The intent of this requirement is for the regulated entity to maintain, keep current, and provide promptly upon request by the regulator *"all information necessary to access and locate records preserved by means of the electronic recordkeeping system."*[15]

SEC 17a-4(f)(3)(iv) and 18a-6(e)(3)(iv):

Organize, maintain, keep current, and provide promptly upon request by the staffs of the Commission, [and other pertinent regulators] having jurisdiction over the [regulated entity] all information necessary to access and locate records preserved by means of the electronic recordkeeping system

This requirement for information to access and locate the records (e.g., unique identifier, index, or properties) is designed to incorporate whatever means a particular electronic recordkeeping system uses to organize the records and locate a specific record.

2.9.2 Compliance Assessment

Cohasset affirms that Google Cloud Storage supports the regulated entity in meeting this SEC requirement to organize, maintain, keep current, and provide promptly the information needed to locate the records.

2.9.3 Google Cloud Storage Capabilities

The regulated entity is responsible for, and Google Cloud Storage supports, compliance with this requirement for information needed to locate the records.

- The records are organized by Bucket name and by record 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, allowing Buckets to be grouped with other Google Cloud resources.
  - The record name can only be assigned during its creation (storage).
    - The record name may include slashes to make objects appear to be organized in a hierarchical structure.
    - For each record, custom name-value pairs, which 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 attributes include:
  - Immutable object attributes, e.g., object name, generation number, creation timestamp, size, and object checksums.

[15] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66424.

- Mutable object attributes, e.g., *Event Hold, Event Hold Release Time, Temporary Hold, Retain Until Time* (for Object Retention Lock) and user-specified attribute tags for records.

- Authorized users can (a) list records in lexicographic order, (b) search the record name, and (c) download attributes as a text file to a designated storage location.
- When record attributes are retrieved (via LIST or GET API calls) the response will include the attributes described above, together with:
  - The dynamically calculated *Retention Expiration Time*, i.e., the earliest date when deletion of a protected record is allowed,
  - The *Event Hold* status (for the indefinite portion of the retention period, such as *while the customer account is open*), and
  - The *Temporary Hold* status (for legal holds, etc.).

  NOTE: If the *Event Hold* status is *True*, the *Retention Expiration Time* will be null, since it cannot be calculated until the event occurs.
- Record attributes are retained for the lifespan of the associated record.

2.9.4 Additional Considerations

In addition, for this requirement, the regulated entity is responsible for:

- Assigning Bucket and record names and other record properties (attributes) to aid in locating records.
- Appropriately managing information, retained separately from Google Cloud Storage, that is needed to access and locate the records.

Additionally, the regulated entity is responsible for: (a) maintaining its account in good standing, (b) authorizing user privileges, and (c) providing requested information to the regulator, in the requested format.

2.10 Designated Executive Officer or Designated Third Party Requirement

2.10.1 Compliance Requirement

SEC 17a-4(f)(3)(v) and 18a-6(e)(3)(v):

(A) Have at all times filed with the [pertinent regulator] the following undertakings with respect to such records signed by either a designated executive officer or designated third party (hereinafter, the "undersigned"):
*****

It is the responsibility of the regulated entity to designate either an executive officer of the firm (Designated Executive Officer) or an unaffiliated third-party (Designated Third Party) to make the required undertaking.

Once the relationship is established, this requirement is the joint responsibility of the regulated entity and the designated party.

In the event the regulated entity fails to download requested records and complete time-stamped audit-trails (if applicable), the designated party is required to promptly furnish the following to the regulator:

- Information deemed necessary by the regulator, and

- Downloaded copies of requested records and complete time-stamped audit-trails (if applicable), in a human readable format and a usable electronic format.

2.10.2 Compliance Assessment

The regulated entity is responsible for (a) designating either an executive officer of the firm or a third-party, (b) obtaining the required undertakings, and (c) submitting the undertaking to its designated examining authority.

2.10.3 Google Cloud Storage Capabilities

Complying with this requirement is the responsibility of the regulated entity.

2.10.4 Additional Considerations

The regulated entity is responsible for complying with this requirement.

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

This section contains a summary assessment of the functionality of Google Cloud Storage, as described in Section 1.3, *Google Cloud Storage Overview and Assessment Scope*, in comparison to CFTC electronic regulatory record requirements. Specifically, this section associates the features described in Section 2, *Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e),* with the principles-based requirements of CFTC Rule 1.31(c)-(d).

Cohasset's assessment, enumerated in Section 2, pertains to the electronic recordkeeping system requirements of SEC Rules 17a-4(f)(2) and 18a-6(e)(2) and the associated SEC interpretations, as well as the audit system requirement of SEC Rules 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii).

In the October 12, 2022, adopting release, the SEC recognizes the CFTC principles-based requirements and asserts a shared objective of ensuring the authenticity and reliability of regulatory records. Moreover, the SEC contends that its two compliance alternatives, i.e., (1) record and audit-trail and (2) non-rewriteable, non-erasable record format, a.k.a. WORM, are more likely to achieve this objective because each alternative requires the specific and testable outcome of accessing and producing modified or deleted records, in their original form, for the required retention period.

> *The proposed amendments to Rules 17a-4 and 18a-6 and the [CFTC] principles-based approach recommended by the commenters share an objective: ensuring the authenticity and reliability of regulatory records. However, the audit-trail requirement is more likely to achieve this objective because, like the existing WORM requirement, it sets forth a specific and testable outcome that the electronic recordkeeping system must achieve: the ability to access and produce modified or deleted records in their original form.*[16] *[emphasis added]*

In Section 2 of this report, Cohasset assesses Google Cloud Storage, with the *Retention* features in *locked* mode, which is a highly restrictive configuration that assures the storage solution applies integrated controls to (a) protect immutability of the record content and certain attributes and (b) prevent deletion over the applied retention period.

In the following table, Cohasset correlates the functionality of Google Cloud Storage, with the *Retention* features in *locked* mode, with the *principles-based* CFTC requirements related to the *form and manner of retention* and the *inspection and production of regulatory records*. In addition, Cohasset contends that Google Cloud Storage, with the *Retention* features in *unlocked* mode, meets these *principles-based* CFTC requirements, when the regulated entity applies appropriate procedural controls to scrutinize actions taken that may allow content to be deleted prior to expiration of the retention period. This less restrictive *unlocked* retention mode provides flexibility to remove or shorten retention periods, which may be beneficial for compliance with privacy and data protection requirements. The first column enumerates the CFTC regulation. The second column provides Cohasset's analysis

[16] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.

and opinion regarding the ability of Google Cloud Storage to meet the requirements for electronic regulatory records in CFTC Rule 1.31(c)-(d).

CFTC 1.31(c)-(d) Regulation [emphasis added]	**Compliance Assessment Relative to CFTC 1.31(c)-(d)**
(c) Form and manner of retention. Unless specified elsewhere in the Act or Commission regulations in this chapter, all regulatory records must be created and retained by a records entity in accordance with the following requirements: *(1) Generally. Each records entity shall retain regulatory records in a form and manner that ensures the authenticity and reliability of such regulatory records in accordance with the Act and Commission regulations in this chapter.* *(2) Electronic regulatory records. Each records entity maintaining electronic regulatory records shall establish appropriate systems and controls that ensure the authenticity and reliability of electronic regulatory records, including, without limitation:* *(i) Systems that maintain the security, signature, and data as necessary to ensure the authenticity of the information contained in electronic regulatory records and to monitor compliance with the Act and Commission regulations in this chapter;*	It is Cohasset's opinion that the CFTC requirements in (c)(1) and (c)(2)(i), for records[17] with time-based and event-based retention periods, are met by the functionality of Google Cloud Storage, with the *Retention* features in *locked* mode, as described in: ● Section 2.2, *Non-Rewriteable, Non-Erasable Record Format* ● Section 2.3, *Record Storage Verification* ● Section 2.4, *Capacity to Download and Transfer Records and Location Information* ● Section 2.8, *Audit System* Additionally, for *records stored electronically*, the CFTC definition of *regulatory records* in 17 CFR § 1.31(a) includes information to access, search and display records, as well as data on records creation, formatting and modification: *Regulatory records means all books and records required to be kept by the Act or Commission regulations in this chapter, including any record of any correction or other amendment to such books and records, provided that, with respect to such books and records stored electronically, regulatory records shall also include:* *(i) Any data necessary to access, search, or display any such books and records; and* *(ii) All data produced and stored electronically describing how and when such books and records were created, formatted, or modified. [emphasis added]* Google Cloud Storage retains immutable attributes (e.g., Global Identifier, generation number, creation timestamp) as an integral component of the records, and, therefore, these attributes are subject to the same retention controls as the associated record. These immutable attributes support both (a) records access, search and display and (b) audit system and accountability for inputting the records. Additionally, mutable attributes stored for records include retention controls and legal hold statuses. The most recent values of mutable attributes are retained for the same time period as the associated records. See Sections 2.4, 2.8 and 2.9 for Google Cloud Storage capabilities related to retaining information needed to search and locate the records. Further, Google Cloud Storage in conjunction with the Google Cloud Storage Cloud Audit Log tracks audit events and provides storage options for retaining this additional audit system information for the same time period as the record. For additional information, see Section 2.8, *Audit System*.

[17] The regulated entity is responsible for retaining and managing any additional required information, such as information to augment search and data on how and when the records were created, formatted, or modified, in a compliant manner.

CFTC 1.31(c)-(d) Regulation [emphasis added]	**Compliance Assessment Relative to CFTC 1.31(c)-(d)**
(ii) Systems that ensure the records entity is able to produce electronic regulatory records in accordance with this section, and ensure the availability of such regulatory records in the event of an emergency or other disruption of the records entity's electronic record retention systems; and	It is Cohasset's opinion that Google Cloud Storage capabilities described in Section 2.5, *Record Redundancy*, including methods for a persistent duplicate copy as well as an alternate source to reestablish the records and associated system attributes, 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*. Additionally, Sections 2.5, *Record Redundancy*, and 2.9, *Information to Access and Locate Records*, explain that all storage classes available to Google Cloud Storage are designed for 11-nines of durability, using erasure coding to store data pieces redundantly across multiple disks located in different power and network failure domains.
(iii) The creation and maintenance of an up-to-date inventory that identifies and describes each system that maintains information necessary for accessing or producing electronic regulatory records.	The regulated entity is required to create and retain an *up-to-date inventory,* as required for compliance with 17 CFR § 1.31(c)(iii).
(d) Inspection and production of regulatory records. Unless specified elsewhere in the Act or Commission regulations in this chapter, a records entity, at its own expense, must produce or make accessible for inspection all regulatory records in accordance with the following requirements: *(1) Inspection. All regulatory records shall be open to inspection by any representative of the Commission or the United States Department of Justice.* *(2) Production of **paper** regulatory records. **** *(3) Production of **electronic** regulatory records.* *(i) A request from a Commission representative for electronic regulatory records will specify a reasonable form and medium in which a records entity must produce such regulatory records.* *(ii) A records entity must produce such regulatory records in the form and medium requested promptly, upon request, unless otherwise directed by the Commission representative.* *(4) Production of **original** regulatory records. ****	It is Cohasset's opinion that Google Cloud Storage has features that support the regulated entity's efforts to comply with requests for inspection and production of records, as described in. ● Section 2.2, *Non-Rewriteable, Non-Erasable Record Format* ● Section 2.4, *Capacity to Download and Transfer Records and Location Information* ● Section 2.6, *Facilities to Produce Records for Examination*, ● Section 2.7, *Provide Records to Regulators* ● Section 2.8, *Audit System* ● Section 2.9, *Information to Access and Locate Records*

4 • Conclusions

Cohasset assessed the functionality of Google Cloud Storage[18] in comparison to the electronic recordkeeping system requirements set forth in SEC Rules 17a-4(f)(2) and 18a-6(e)(2) and described features that support the regulated entity as it meets the requirements of SEC Rules 17a-4(f)(3) and 18a-6(e)(3).

Cohasset determined that Google Cloud Storage, when properly configured, has the following functionality, which meets the regulatory requirements:

- Retains records and immutable system attributes in non-rewriteable, non-erasable format, for time-based and event-based retention periods, by applying the *Google Cloud Storage Retention* features in *locked* mode.
- Applies *Temporary Hold* attributes to preserve records for a subpoena, legal hold or similar circumstances.
- Prohibits deletion of records until the *Retention Expiration Time* and *Retain Until Time* are in the past and any applied *Temporary Holds* and *Event Holds* are removed.
- Verifies the accuracy of the recording processes which utilize checksums and Google Cloud Storage validation processes.
- Provides authorized users with the capacity and tools to find and download the record and information needed to locate the records for a browser or other local tool to render a human-readable view and produce it in the requested electronic format.
- Maintains records redundancy to either retrieve a duplicate or regenerate an accurate replica of the record from erasure coded data should an error occur, or an availability problem be encountered.

Additionally, Google Cloud Storage supports the regulated entity's compliance with the requirements defined in SEC Rules 17a-4(f)(3) and 18a-6(e)(3), by (a) retaining an audit system for non-rewriteable, non-erasable records by storing immutable attributes related to inputting each record and downloading these attributes with the associated record, (b) furnishing facilities to produce records for examination, (c) providing (transferring) records to the regulator for examination, and (d) maintaining information to access and locate the record.

Accordingly, Cohasset concludes that Google Cloud Storage, when properly configured and the additional considerations are satisfied, meets the electronic recordkeeping system requirements of SEC Rules 17a-4(f)(2) and 18a-6(e)(2) and FINRA Rule 4511(c), as well as supports the regulated entity in its compliance with the requirements in SEC Rules 17a-4(f)(3) and 18a-6(e)(3). In addition, the assessed capabilities meet the principles-based electronic records requirements of CFTC Rule 1.31(c)-(d).

[18] See Section 1.3, *Google Cloud Storage Overview and Assessment Scope*, for an overview of the solution and the scope of deployments included in the assessment.

Appendix A • Overview of Relevant Electronic Records Requirements

This section establishes the context for the regulatory requirements that are the subject of this assessment by providing an overview of the regulatory foundation for electronic records retained on compliant electronic recordkeeping systems.

A.1 Overview of SEC Rules 17a-4(f) and 18a-6(e) *Electronic Recordkeeping System* Requirements

In 17 CFR §§ 240.17a-3 and 240.17a-4 for securities broker-dealer industry and 17 CFR §§ 240.18a-5 and 240.18a-6 for nonbank SBS entities, the SEC stipulates recordkeeping requirements, including retention periods.

Effective January 3, 2023, the U.S. Securities and Exchange Commission (SEC) promulgated amendments[19] to 17 CFR § 240.17a-4 (Rule 17a-4) and 17 CFR § 240.18a-6 (Rule 18a-6), which define more technology-neutral requirements for electronic recordkeeping systems.

> *The objective is to prescribe rules that remain workable as record maintenance and preservation technologies evolve over time but also to set forth requirements designed to ensure that broker-dealers and SBS Entities maintain and preserve records in a manner that promotes their integrity, authenticity, and accessibility.*[20] [emphasis added]

These 2022 amendments (a) provide a record and complete time-stamped audit-trail alternative and (b) allow regulated entities to continue using the electronic recordkeeping systems they currently employ to meet the non-rewriteable, non-erasable (i.e., WORM or write-once, read-many) requirement.

> *Under the final amendments, broker-dealers and nonbank SBS Entities have the flexibility to preserve all of their electronic Broker-Dealer Regulatory Records or SBS Entity Regulatory Records either by: (1) using an electronic recordkeeping system that meets either the audit-trail requirement or the WORM requirement; or (2) preserving some electronic records using an electronic recordkeeping system that meets the audit-trail requirement and preserving other electronic records using an electronic recordkeeping system that meets the WORM requirement.*[21] [emphasis added]

The following sections separately address (a) the record and audit-trail and (b) the non-rewriteable, non-erasable record format alternatives for compliant electronic recordkeeping systems.

A.1.1 Record and Audit-Trail Alternative

The objective of this requirement is to allow regulated entities to keep required records and complete time-stamped record audit-trails in business-purpose recordkeeping systems.

---

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

20 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66428.

21 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66419.

> *[T]o preserve Broker-Dealer Regulatory Records and SBS Regulatory Records, respectively, on the same electronic recordkeeping system they use for business purposes, but also to require that the system have the capacity to recreate an original record if it is modified or deleted. This requirement was designed to provide the same level of protection as the WORM requirement, which prevents records from being altered, over-written, or erased.*[22] [emphasis added]

The complete time-stamped audit-trail must both (a) establish appropriate systems and controls that ensure the authenticity and reliability of required records and (b) achieve the testable outcome of accessing and reproducing the original record, if modified or deleted during the required retention period, without prescribing how the system meets this requirement.

> *[L]ike the existing WORM requirement, [the audit-trail requirement] sets forth a specific and testable outcome that the electronic recordkeeping system must achieve: the ability to access and produce modified or deleted records in their original form.*[23] [emphasis added]

Further, the audit-trail applies only to required records: *"the audit-trail requirement applies to the final records required pursuant to the rules, rather than to drafts or iterations of records that would not otherwise be required to be maintained and preserved under Rules 17a-3 and 17a-4 or Rules 18a-5 and 18a-6."*[24] [emphasis added]

A.1.2 Non-Rewriteable, Non-Erasable Record Format Alternative

With regard to the option of retaining records in a non-rewriteable, non-erasable format, the adopting release clarifies that the previously released interpretations to both SEC Rules 17a-4(f) and 18a-6(e) still apply.

> *The Commission confirms that a broker-dealer or nonbank SBS Entity can rely on the 2003 and 2019 interpretations with respect to meeting the WORM requirement of Rule 17a-4(f) or 18a- 6(e), as amended.*
> *****
> *In 2001, the Commission issued guidance that Rule 17a-4(f) was consistent with the ESIGN Act. The final amendments to Rule 17a-4(f) do not alter the rule in a way that would change this guidance. Moreover, because Rule 18a-6(e) is closely modelled on Rule 17a-4(f), it also is consistent with the ESIGN Act****[25] [emphasis added]

In addition to the Rules, the following interpretations are extant and apply to both SEC Rules 17a-4(f) and 18a-6(e).

- *Commission Guidance to Broker-Dealers on the Use of Electronic Storage Media Under the Electronic Signatures in Global and National Commerce Act of 2000 With Respect to Rule 17a-4(f), Exchange Act Release No. 44238 (May 1, 2001), 66 FR 22916 (May 7, 2001)* (2001 Interpretative Release).
- *Electronic Storage of Broker-Dealer Records, Exchange Act Release No. 47806 (May 7, 2003), 68 FR 25281, (May 12, 2003)* (2003 Interpretative Release).
- *Recordkeeping and Reporting Requirements for Security-Based Swap Dealers, Major Security Based Swap Participants, and Broker-Dealers, Exchange Act Release No. 87005 (Sept. 19, 2019), 84 FR 68568 (Dec. 16, 2019)* (2019 SBSD/MSBSP Recordkeeping Adopting Release).

---

22 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.
23 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.
24 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66418.
25 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66419.

The 2003 Interpretive Release allows rewriteable and erasable media to meet the non-rewriteable, non-erasable requirement, if the system delivers the prescribed functionality, using appropriate integrated control codes.

> *A broker-dealer would not violate the requirement in paragraph* [(f)(2)(i)(B) (refreshed citation number)] *of the rule if it used an electronic storage system that prevents the overwriting, erasing or otherwise altering of a record during its required retention period through the use of integrated hardware and software control codes.*[26] [emphasis added]

Further, the 2019 interpretation clarifies that solutions using only software control codes also meet the requirements of the Rules:

> *The Commission is clarifying that a software solution that prevents the overwriting, erasing, or otherwise altering of a record during its required retention period would meet the requirements of the rule.*[27] [emphasis added]

The term *integrated* means that the method used to achieve non-rewriteable, non-erasable preservation must be an integral part of the system. The term *control codes* indicates the acceptability of using attribute codes (metadata), which are integral to the software controls or the hardware controls, or both, which protect the preserved record from overwriting, modification or erasure.

The 2003 Interpretive Release is explicit that merely mitigating (rather than preventing) the risk of overwrite or erasure, such as relying solely on passwords or other extrinsic security controls, will not satisfy the requirements.

Further, the 2003 Interpretive Release requires the capability to retain a record beyond the SEC-established retention period, when required by a subpoena, legal hold or similar circumstances.

> *[A] broker-dealer must take appropriate steps to ensure that records are not deleted during periods when the regulatory retention period has lapsed but other legal requirements mandate that the records continue to be maintained, and the broker-dealer's storage system must allow records to be retained beyond the retentions periods specified in Commission rules.*[28] [emphasis added]

See Section 2, *Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e),* for each SEC electronic recordkeeping system requirement and a description of the functionality of Google Cloud Storage related to each requirement.

A.2 Overview of FINRA Rule 4511(c) *Electronic Recordkeeping System* Requirements

Financial Industry Regulatory Authority (FINRA) rules regulate member brokerage firms and exchange markets. Additionally, FINRA adopted amendments clarifying the application of FINRA rules to security-based swaps (SBS).[29]

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

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

---

26 2003 Interpretative Release, 68 FR 25282.

27 Recordkeeping and Reporting Requirements for Security-Based Swap Dealers, Major Security- Based Swap Participants, and Broker-Dealers, Exchange Act Release No. 87005 (Sept. 19, 2019), 84 FR 68568 (Dec. 16, 2019) (2019 SBSD/MSBSP Recordkeeping Adopting Release).

28 2003 Interpretative Release, 68 FR 25283.

29 FINRA, Regulatory Notice 22-03 (January 20, 2022), FINRA Adopts Amendments to Clarify the Application of FINRA Rules to Security-Based Swaps.

A.3 Overview of CFTC Rule 1.31(c)-(d) *Electronic Regulatory Records* Requirements

Effective August 28, 2017, the Commodity Futures Trading Commission (CFTC) amended 17 CFR § 1.31 (CFTC Rule) to modernize and make technology-neutral the form and manner in which to keep regulatory records. This resulted in less-prescriptive, principles-based requirements.

> *Consistent with the Commission's emphasis on a less-prescriptive, principles-based approach, proposed § 1.31(d)(1) would rephrase the existing requirements in the form of a general standard for each records entity to retain all regulatory records in a form and manner necessary to ensure the records' and recordkeeping systems' authenticity and reliability.*[30] [emphasis added]

The following definitions in 17 CFR § 1.31(a) confirm that recordkeeping obligations apply to all *records entities* and all *regulatory records*. Further, for *electronic regulatory records*, paragraphs (i) and (ii) establish an expanded definition of an electronic regulatory record to include information describing data necessary to access, search and display records, as well as information describing how and when such books and records were created, formatted, or modified.

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

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

> *Duration of retention. Unless specified elsewhere in the Act or Commission regulations in this chapter:*
>
> *(1) A records entity shall keep regulatory records of any swap or related cash or forward transaction (as defined in § 23.200(i) of this chapter), other than regulatory records required by § 23.202(a)(1) and (b)(1)-(3) of this chapter, from the date the regulatory record was created until the termination, maturity, expiration, transfer, assignment, or novation date of the transaction and for a period of not less than five years after such date.*
>
> *(2) A records entity that is required to retain oral communications, shall keep regulatory records of oral communications for a period of not less than one year from the date of such communication.*
>
> *(3) A records entity shall keep each regulatory record other than the records described in paragraphs (b)(1) or (b)(2) of this section for a period of not less than five years from the date on which the record was created.*
>
> *(4) A records entity shall keep regulatory records exclusively created and maintained on paper readily accessible for no less than two years. A records entity shall keep electronic regulatory records readily accessible for the duration of the required record keeping period.* [emphasis added]

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

[30] Recordkeeping, 82 FR 24482 (May 30, 2017) (2017 CFTC Adopting Release).

Appendix B • Cloud Provider Undertaking

B.1 Compliance Requirement

Separate from the electronic recordkeeping system requirements described in Section 2, *Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e),* the SEC requires submission of an undertaking when records are stored on systems owned or operated by a party other than the regulated entity.

The purpose of the undertaking is to ensure the records are accessible and can be examined by the regulator.

SEC Rules 17a-4(i)(1)(ii) and 18a-6(f)(1)(ii) explain an 'Alternative Undertaking,' which applies to cloud service providers if the regulated entity has 'independent access' to records, which allows it to (a) regularly access the records without relying on the cloud service provider to take an intervening step to make the records available, (b) allow regulators to examine the records, during business hours, and (c) promptly furnish the regulator with true, correct, complete and current hard copy of the records.

This undertaking requires the cloud service provider (a) facilitate the process, (b) not block access, and (c) not impede or prevent the regulated entity or the regulator itself from accessing, downloading, or transferring the records for examination.

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

SEC 17a-4(i)(1)(ii) and 18a-6(f)(1)(ii):

(A) If the records required to be maintained and preserved pursuant to the provisions of [§ 240.17a-3 or § 240.18a-5] and this section are maintained and preserved by means of an electronic recordkeeping system as defined in paragraph [(f) or (e)] of this section utilizing servers or other storage devices that are owned or operated by an outside entity (including an affiliate) and the [regulated entity] has independent access to the records as defined in paragraph [(i)(1)(ii)(B) or (f)(1)(ii)(B)] of this section, the outside entity may file with the Commission the following undertaking signed by a duly authorized person in lieu of the undertaking required under paragraph [(i)(1)(i) or (f)(1)(i)] of this section:

> The undersigned hereby acknowledges that the records of [regulated entity] are the property of [regulated entity] and [regulated entity] has represented: one, that it is subject to rules of the Securities and Exchange Commission governing the maintenance and preservation of certain records, two, that it has independent access to the records maintained by [name of outside entity], and, three, that it consents to [name of outside entity or third party] fulfilling the obligations set forth in this undertaking. The undersigned undertakes that [name of outside entity or third party] will facilitate within its ability, and not impede or prevent, the examination, access, download, or transfer of the records by a representative or designee of the Securities and Exchange Commission as permitted under the law. *****

(B) A [regulated entity] utilizing servers or other storage devices that are owned or operated by an [outside entity or third party] has independent access to records with respect to such [outside entity or third party] if it can regularly access the records without the need of any intervention of the [outside entity or third party] and through such access:

(1) Permit examination of the records at any time or from time to time during business hours by representatives or designees of the Commission; and

(2) Promptly furnish to the Commission or its designee a true, correct, complete and current hard copy of any or all or any part of such records [emphasis added]

agreed to in the Traditional Undertaking. Rather, it means that the third party undertakes to provide to the Commission representative or designee or SIPA trustee the same type of technical support with respect to records access that it would provide to the broker-dealer or SBS Entity in the normal course.[31] [emphasis added]

B.2 Google Undertaking Process

- To obtain an Alternative Undertaking for Google Cloud Storage, the regulated entity contacts its Google Account Representative to complete the process.
- Google will prepare the undertaking, utilizing the explicit language in the Rule, and provide the undertaking to the regulated entity.
  - IMPORTANT NOTE: This action by Google does not relieved the regulated entity from its responsibility to prepare and maintain required records.

B.3 Additional Considerations

The regulated entity is responsible for (a) initiating the undertaking, (b) maintaining its account in good standing, (c) implementing and configuring the cloud services to ensure its records are maintained and preserved as required by applicable laws and regulations, (f) maintaining technology, encryption keys and privileges to access Google Cloud Storage, and (g) assuring that the regulator has (when needed) access privileges, encryption keys, and other information and services to permit records to be accessed, downloaded, and transferred.

[31] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66429.

About Cohasset Associates, Inc.

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

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

Management Consulting: Cohasset strategizes with its multi-national and domestic clients, designing and supporting implementations that promote interdisciplinary information governance, achieve business objectives, optimize information value, improve compliance, and mitigate information-related risk.

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

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

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

For domestic and international clients, Cohasset:

- *Formulates information governance implementation strategies*
- *Develops policies and standards for records management and information governance*
- *Creates clear and streamlined retention schedules*
- *Prepares training and communications for executives, the RIM network and all employees*
- *Leverages content analytics to improve lifecycle controls for large volumes of eligible information, enabling clients to classify information, separate high-value information and delete what has expired*
- *Designs and supports the implementation of information lifecycle practices that mitigate the cost and risk associated with over-retention*
- *Defines strategy and design for information governance in collaboration tools, such as M365*
- *Defines technical and functional requirements and assists with the deployment of enterprise content management and collaboration tools*

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