Cohasset Associates

Google Cloud Backup and DR Service

COMPLIANCE ASSESSMENT

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

Abstract

Google Cloud Backup and DR Service™ is a secure, isolated, and specialized cloud-first backup and disaster recovery storage solution to protect workloads running in Google Cloud by storing backups in secure storage. The minimum enforced retention period is designed to meet securities industry requirements for preserving records in non-rewriteable, non-erasable format for the applied retention period and legal holds.

In this report, Cohasset Associates, Inc. (Cohasset) assesses the functionality of Google Cloud Backup and DR Service (see Section 1.3, *Google Cloud Backup and DR Service 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 Backup and DR Service, when properly configured with a minimum enforced retention period on the backup vault and other compliance capabilities, 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)(iii) and 18a-6(e)(3)(iii). Additionally, the assessed functionality of Google Cloud Backup and DR Service 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.

February 2025

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 Backup and DR Service 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 14

2.4 Capacity to Download and Transfer Records and Location Information 15

2.5 Record Redundancy 17

2.6 Audit System 18

3 • Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d) **20**

4 • Conclusions **23**

Appendix A • Overview of Relevant Electronic Records Requirements **24**

A.1 Overview of SEC Rules 17a-4(f) and 18a-6(e) *Electronic Recordkeeping System* Requirements 24

A.2 Overview of FINRA Rule 4511(c) *Electronic Recordkeeping System* Requirements 26

A.3 Overview of CFTC Rule 1.31(c)-(d) *Electronic Regulatory Records* Requirements 27

Appendix B • Cloud Provider Undertaking **28**

B.1 Compliance Requirement 28

B.2 Google Undertaking Process 29

B.3 Additional Considerations 29

About Cohasset Associates, Inc. **30**

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 Backup and DR Service 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 the Google Cloud Backup and DR Service 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 Backup and DR Service, in comparison to the electronic recordkeeping system requirements of SEC Rules 17a-4(f)(2) and 18a-6(e)(2) and describe audit system features that support the regulated entity in its compliance with SEC Rules 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii); 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 Backup and DR Service; 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 Backup and DR Service and its functionality or other Google products or services. The information utilized by Cohasset to conduct this assessment consisted of: (a) oral discussions, (b) product demonstrations, including system setup and configuration, (c) system documentation, (d) user and system administrator guides, and (e) 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 Backup and DR Service Overview and Assessment Scope

1.3.1 Google Cloud Backup and DR Service Overview

Google Cloud Backup and DR Service captures a point-in-time *backup*[4] of a resource (e.g., a database, file system, or virtual machine) to reestablish the archived records. The *backup* is retained immutably and indelibly according to the configuration defined in the backup vault, which applies integrated retention controls to retain the backups and associated records in compliance with securities industry electronic record-keeping requirements; see Figure 1, Logical Architecture.

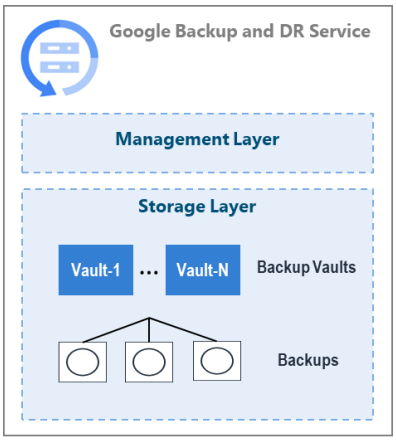

Figure 1: Logical Architecture

This report assesses Google Cloud Backup and DR Service, running the following software:

- **Management Layer** centralizes the management of backups and associated metadata for designated workloads.
  - **Workloads** are Google Cloud Services, e.g., databases and Compute Engine virtual machines, including: https://cloud.google.com/backup-disaster-recovery/docs/concepts/backup-dr#backup_plans
- **Backup vaults** securely store backups separate from the resource instance. For compliance with the Rule, the backup vault must be appropriately configured with a minimum enforced retention period.

1.3.2 Assessment Scope

The scope of this Compliance Assessment Report is focused specifically on the compliance-related capabilities of Google Cloud Backup and DR Service.

[4] The SEC uses the phrase *books and records* to describe information that must be retained for regulatory compliance. In this report, Cohasset uses the term Backup to refer to a *collection of records* and to recognize that the content of the *backup* may be required for regulatory compliance.

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 Backup and DR Service, 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 audit system requirement of SEC Rules 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii).

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 Backup and DR Service
- ***Google Cloud Backup and DR Service 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 Backup and DR Service, as described in Section 1.3, *Google Cloud Backup and DR Service 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.*[5] [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.*[6] [emphasis added]

2.1.2 Compliance Assessment

In this report, Cohasset has not assessed Google Cloud Backup and DR Service 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 Backup and DR Service, with the features and controls described in Sections 2.2 through 2.6 of this report.

Reminder: This requirement pertains to the regulated entity's business-purpose data processing system (i.e., a trading system), when configured to retain the record and its complete time-stamped audit trail. This requirement is an alternative to the more stringent 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

2.2.1 Compliance Requirement

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

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.

5 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.

6 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66418.

> *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 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.*[7] [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.*[8] [emphasis added]

2.2.2 Compliance Assessment

It is Cohasset's opinion that the functionality of Google Cloud Backup and DR Service, when the backup vault is configured with a minimum enforced retention period, meets this SEC requirement to retain records in non-rewriteable, non-erasable format for the applied time-based[9] 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 non-rewriteable, non-erasable record format requirement is a more stringent alternative to the complete time-stamped audit-trail requirement, which is addressed in Section 2.1.

2.2.3 Google Cloud Backup and DR Service Capabilities

This section describes the functionality of Google Cloud Backup and DR Service 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

Google Cloud Backup and DR Service centralizes the management of backups and associated metadata, stored in backup vaults on the Google Cloud infrastructure.

---

7 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66419.

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

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

To meet this SEC Rule 17a-4(f) requirement, Google Cloud Backup and DR Service:

- Backup vaults must be configured with a minimum enforced retention period set in days. Optionally, the backup vaults minimum enforced retention period may be *Locked,* which prevents reducing of the specified value once the *Lock* effective date is in the past.
- Backup plans (which may consist of templates and profiles) must be configured to store backups in a backup vault location with an appropriate minimum enforced retention period.

The following table summarizes the controls applied when a backup's retention expiration date has not been reached. See the subsections following this *Overview*, for information on configuring the retention features and the resulting integrated controls.

	Backup Vault with Minimum Enforced Retention Period
Protecting record content and immutable metadata	● By design, the contents of a backup and its immutable metadata (i.e. metadata governing the backup content) cannot be modified for its stored lifespan, as a fundamental feature of Google Cloud Backup and DR Service. ● Therefore, the contents of the collection of records and record metadata stored in the backup are protected and cannot be modified for its stored lifespan.
Restricting changes to retention controls	● A backup's calculated retention expiration date cannot be reduced or removed, though it can be extended. ● Optionally, when configured with the *Lock* feature and the *Lock* effective date in the past, a backup vault's minimum enforced retention period cannot be reduced or removed, though it can be extended. ● See Section 2.2.3.3, *Backup Definition and Retention Controls.*
Applying and removing legal holds	● For backups that must be preserved for a duration longer than the calculated retention expiration date, the backup's retention expiration date may be extended, using the application programming interface, for select backups that are subject to the hold. ● See Section 2.2.3.4, *Legal Holds (Temporary Holds)*, for additional information.
Restricting deletion	● Attempts by any user to **delete** a backup prior to expiration of its retention controls are rejected. ● See Section 2.2.3.5, *Deletion Controls*, for additional information.

2.2.3.2 Retention-related Configurations

► To be compliant with the Rule, Google Cloud Backup and DR Service must be properly configured, which requires settings for both the (a) backup vault and (b) backup plan.

- The **backup vault** is a secure storage location for storing backups separate from the source.
- The **backup plan** is composed of backup policies and configurations, which govern the backup timing, frequency, standard retention, and other actions for creating and managing backups and the resource profile, which determines the physical location where the backup is stored.

The following table lists the retention-related configurations for the (a) backup vault and (b) backup plan.

	Backup Vault - Retention-related Configurations
Backup Vault Name	● The name of the backup vault where backups will be stored.
Minimum enforced retention period	● The minimum retention expiration period that the backup vault retains backups. The minimum protection time is 1 day, and the maximum is 36,135 days. Note: This period can be reduced or extended until the *Lock* effective date (see row below) is in the past. After the *Lock* effective date is past, this period can only be extended.

***Lock* feature**	● This optional feature may be enabled to prevent the backup vaults minimum enforced retention period from being reduced. Note: The *Lock* feature is not required for compliance with the Rule, since each backup is assigned a retention period which can only be extended and never reduced.
***Lock* effective date**	● The date after which the *Lock* feature is permanently enforced on the backup vault, and the minimum enforced retention period is *Locked,* meaning it cannot be reduced, though it may be extended.
	Backup Plan - Retention-related Configurations
Backup Plan	● The backup plan name is a unique alpha-numeric name ● The backup plan description contains a brief description of the template and its purpose. ● The backup plan specifies the backup frequency (e.g., daily), the days of the week that backups are performed, the start and end times for backup operations, the backup vault where backups will be stored and managed and the retention (auto-delete) period after which the backups are auto-deleted, and replication of the backups to other locations or storage pools for redundancy and disaster recovery. *Users apply backup plans to protect desired resources.* Notes: ○ The backup plan retention (auto-delete) period does not specify a required period during which the backup must be kept; instead, it defines when auto-deletion will occur. Thus, a backup may be manually deleted prior to expiration of the retention (auto-delete) period. ○ The backup plan retention (auto-delete) period must equal or be longer than (and cannot be shorter than) the backup vault's minimum enforced retention period. This eliminates conflicts which would result in attempts to auto-delete based on a period that is shorter than the minimum enforced retention period. ○ Since the backup plan's retention (auto-delete) period does not require retention, this period is not relied upon for compliance with the Rule. Instead see the minimum enforced retention period set for the backup vault, as explained above.

2.2.3.3 Backup Definitions and Retention Controls

- Backup vaults securely store backups separate from the primary resource.
- Each backup is considered a separate record and is comprised of:
  - The complete immutable content, which contains a collection of records and record metadata.
  - *Immutable* attributes, including (a) the Google cloud project ID, (b) Google Cloud location, (c) backup vault ID, (d) data source ID, (e) backup ID, and (f) creation timestamp.
  - *Mutable* attributes, which include the retention expiration date.
- The calculated retention expiration date is applied to the backup using the current backup vault settings. Specifically, the retention expiration date is calculated by adding the backup vault's minimum enforced retention period to the backup's creation timestamp.
- Additionally, the backup plan specifies a retention (auto-delete) period, which does not set a requirement to keep the backup and, instead, sets an auto-delete period. Accordingly, a backup will be auto-deleted upon expiration of the retention (auto-delete) period, though it may be manually deleted at any time.
- The following table summarizes the interaction of the (a) retention controls applied to a backup by the backup vault settings and (b) auto-deletion actions applied by the backup plan's retention (auto-deletion) period.

Retention Periods	Retention Controls
Backup vault's minimum enforced retention period matches the backup plan's retention (auto-delete) period	• The minimum enforced retention period and calculated retention expiration date are stored, based on the backup vaults minimum enforced retention period. • Backups are eligible for deletion upon expiration of the calculated retention expiration date, which is stored in the backups metadata. • Auto-delete actions will delete the backups, when they become eligible, if the two periods match.
Backup vault's minimum enforced retention period is shorter than the backup plan's retention (auto-delete) period	• The minimum enforced retention period and calculated retention expiration date are stored, based on the backup vaults minimum enforced retention period. • Backups are eligible for deletion upon expiration of the calculated retention expiration date, which is stored in the backup's metadata. • Auto-delete actions will delete the backups when the backup plan's retention (auto-delete) period expires, which is after the backup is eligible, since the backup vaults minimum enforced retention period is shorter than the backup plan's retention (auto-delete) period.
Backup vault's minimum enforced retention period is longer than the backup plan's retention (auto-delete) period	• When resources are initially configured for protection by the Backup and DR service, validations are performed to detect and prohibit protections where a backup vault's minimum enforced retention period would be longer than the backup plan's retention (auto-delete) period. If such scenarios do occur (e.g. due to subsequent updates of the originally configured values), Backup and DR service will create backups having enforced retention set to the higher of the two values defined by: (1) the backup vault's minimum enforced retention period, and (2) the backup plan's retention (auto-delete) period.

► The following table describes the integrated retention controls that are applied to each backup stored in a backup vault with a minimum enforced retention period. In addition, the row entitled *Modifying or removing retention controls* explains allowed and prevented changes to the (a) retention controls applied to a backup by the backup vault settings and (b) auto-deletion actions applied by the plan's retention (auto-deletion) period.

	Enforced Retention Period
Terminology	• **Backup Plan** defines what resources will be backed up, the backup vault location, backup frequency and retention and replication details. The Backup Plan may be optionally configured with a *Retain For* (deletion date/time). The backup vault configuration always takes precedence for retention time, if there is a conflict between the backup vault settings and the 'backup configurations' in the Backup Plan. • Each **backup** is a point-in-time archival copy of the original source and provides a recovery point to reestablish the archived backup and the collection of records and record metadata stored in the backup. • **Backup vault** is the name of the secure storage location and where the minimum enforced retention period is set. Additionally, the *Lock* feature may be enabled and configured with a *Lock* effective date, which prevents reductions to the backup vault minimum enforced retention period once the *Lock* effective date is in the past. • **Backup retention expiration date** is derived from adding the backup vault's minimum enforced retention period to the backup's creation timestamp and is stored as an attribute of the backup. • Each backup stores a **collection of records and record metadata**[10], i.e., point-in-time record archives.

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

	Enforced Retention Period
Protecting record content and associated metadata	• A collection of records and associated record metadata are retained within the backup, and each backup is inherently read-only and unchangeable. Therefore, the backup content (i.e., the collection of records, record names and other record metadata) cannot be changed over the lifespan of the backup. • Each backup is a point-in-time archival copy and, by design, cannot be overwritten or modified. • The backup unique identifier, resource (source system) backed up, and backup creation timestamp are immutable for the lifespan of the backup. • Mutable backup metadata includes the calculated retention expiration date, which may be extended (deferred to a later date) but not reduced (set to an earlier date).
Modifying or removing retention controls	• When compliant retention controls (i.e., minimum enforced retention period) are configured for a backup vault, they are applied to all new backups stored in the backup vault. • When compliant retention controls are applied to a specific backup vault, the retention expiration date, calculated using the minimum enforced retention period, is stored as metadata for the backup. The backups calculated retention expiration date cannot be reduced (set to an earlier date), though it may be extended (deferred to a later date). • The backup plan's retention (auto-delete) period may be reduced or extended. See the "Retention Controls" table above for details regarding associated scenarios. Reminder: The backup plan's retention (auto-delete) period does not set a requirement to keep the backup and, instead, sets an auto-delete period.
Applying legal holds	• The retention expiration date may be extended for select backups that are subject to the hold. • See Section 2.2.3.4, *Legal Holds (Temporary Holds),* for additional information.
Restricting deletion	• A specific backup, and its associated records, are eligibility for deletion only when the retention expiration date applied to the backup is in the past. • Any attempt to delete a backup that is not eligible is rejected. • See Section 2.2.3.3, *Deletion Controls*, for additional information.
Moving Backup copies	• Backups cannot be moved from the backup vault where they were originally created and stored. • Accordingly, retention controls cannot be circumvented by moving a backup to a backup vault with different retention controls.
Displaying retention controls	• To aid the user, the minimum enforced retention period and *Lock* status can be viewed in the backup vault settings.
Accessing records	• To access the contents (collection of records and record metadata) stored within a backup, the backup can be restored. • Also see Section 2.4, *Capacity to Download and Transfer Records and Location Information.*

2.2.3.4 Legal Holds (Temporary Holds)

When litigation or a subpoena requires records to be placed on hold, which could entail retaining them beyond their assigned retention expiration date, the regulated entity must ensure the subject records (contained in associated backups) are protected for the duration of the hold.

- A backup's retention expiration date may be extended, using the application programming interface, for select backups that are subject to the hold.
- If the extension of the retention expiration date is insufficient, it must continue being extended to meet the legal hold requirements.

2.2.3.5 Deletion Controls

- The backup may be deleted when the retention expiration date is in the past.
  - Deletion of eligible backups may be initiated manually by authorized users or automatically by automated cleanup processes, using the backup plan's retention (auto-delete) period.
  - Attempts to delete a backup that is ineligible for deletion will be rejected.
- The deletion of a backup, when eligible, does not impact the recoverability of any backups still under retention.
- Deletion of a backup vault is prohibited, unless it is empty.

2.2.3.6 Security in Google Cloud Backup and DR Service

In addition to the stringent retention protection, management and security controls described above, Google Cloud Backup and DR Service includes the following security capabilities that support retention of authentic and reliable records.

- Google Cloud Backup and DR Service, including the backup vault storage feature, is designed to meet enterprise security and compliance requirements. For each backup vault, authorized users apply and manage permissions using Google Cloud Identity and Access Management (IAM).
  - IAM manages permissions governing which principals can access or modify backup vault data. Backup vault principals are typically end user Google accounts.
- Secure socket layer (SSL) policies may be configured to specify a minimum transport layer security (TLS) 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 applications to negotiate SSL.
  2. **Modern:** Supports a wide set of SSL features, allowing modern source applications 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.
- Backup data is encrypted:
  - When Hyper Text Transfer Protocol is performed; Google Cloud Backup and DR Service uses transport-layer encryption (HTTPS) to protect against data leakage over shared networks.
  - Google Cloud Backup and DR Service encrypts data at rest and automatically decrypts the data, to render it for use.
  - The regulated entity may encrypt records prior to uploading to Google Cloud Backup and DR Service. 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. More information is available at https://cloud.google.com/security/compliance.

2.2.3.7 Clock Management

- Google Cloud Backup and DR Service, including the service components supporting the backup vault feature, uses Google Cloud's internal system clock. This system clock cannot be modified by end users and, therefore, cannot be manipulated to circumvent the timestamp-driven protections provided by the backup vault's enforced retention features.

2.2.4 Additional Considerations

In addition, for this non-rewriteable, non-erasable record format requirement, the regulated entity is responsible for:

- Configuring the backup vault with the appropriate minimum enforced retention period.
- Ensuring that backups required to comply with the Rule are stored in the properly configured backup vaults.
- Extending selected backups' retention expiration date, using the application programming interface, as appropriate, to preserve backups needed for legal matters, government investigations, external audits and other similar circumstances.
- Creating and storing backups in a backup vault within 24 hours of record creation to assure records are captured. Note: A backup may store multiple days' records; however, longer timespans between record creation and backup creation may result in backups that reflect changes and deletions made on the source records.
- Storing records requiring event-based[11] retention periods in a separate compliant system or otherwise planning for event-based retention, since Google Cloud Backup and DR Service does not currently support event-based retention periods.
- Additionally, the regulated entity is responsible for: (a) maintaining its account in good standing and paying for appropriate services to allow backups to be retained until the applied retention expiration date has expired or until the records have been transferred to another compliant storage system, (b) maintaining the source system and information needed to locate, read and interpret the downloaded copy of the backups from Google Cloud Backup and DR Service, (c) authorizing user privileges, and (d) maintaining appropriate technology, encryption keys, and other information and services needed to retain the records.

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.

[11] 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.

2.3.2 Compliance Assessment

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

2.3.3 Google Cloud Backup and DR Service Capabilities

The recording and post-recording verification processes of Google Cloud Backup and DR Service are described below.

2.3.3.1 Recording Process

- Google Cloud Backup and DR Service performs validation processes during the recording process (e.g., computing and recording an immutable checksum for a randomly-selected sample of the data associated with that backup).

2.3.3.2 Post-Recording Verification Process

- Post-recording verification is continuously performed to validate that backup data still matches what was originally recorded. For example, when backup data is accessed (i.e. during restore operations), a new checksum may be calculated and compared to the previously stored, immutable checksum value. If the checksum values do not match (indicating that data has changed), then the corresponding operation will fail and will generate a corresponding error notification.

2.3.4 Additional Considerations

- The source system is responsible for transmitting the complete contents of the required records. Google Cloud Backup and DR Service validates the accuracy of its recording process.

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

Cohasset asserts that the functionality of Google Cloud Backup and DR Service meets this SEC requirement to maintain capacity to readily download and transfer the records and information in Google Cloud Backup and DR Service used to locate the records, when the considerations described in Section 2.4.4 are satisfied.

2.4.3 Google Cloud Backup and DR Service Capabilities

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

- Google Cloud Backup and DR Service assures each backup is assigned a unique identifier comprised of the following attributes, which facilitate findability:
  - Each backup is uniquely identified by the combination of (a) the Google cloud project ID, which is unique across the entire Google Cloud namespace, (b) a Google Cloud location, (c) a backup vault ID, which is unique within the specified project, (d) a data source ID, specifying the specific resource being backed up, (e) a backup ID, which is unique within the specified data source, and (f) a creation timestamp corresponding to the time the backup was captured.
  - Google Cloud Backup and DR Service immutably retains this metadata for the duration of the applied retention period.
- Using Google Cloud Backup and DR Service, the regulated entity can search the contents (i.e., the collection of records and record metadata stored in the backup) by recovering a point in time backup to local resources. Once recovered the regulated entity can search for records using local metadata.
- Each backup contains the then-current record contents. To isolate the records added, deleted or changed, two backups are restored and compared, in a location other than Google Cloud Backup and DR Service.
- Google Cloud Backup and DR Service, supported by the underlying Google Cloud infrastructure services, assures that hardware and software capacity allows for ready access to the backups and metadata attributes. Further, Google Cloud maintains redundant storage media, network, and power to mitigate outages that would result in unavailability of data.

2.4.4 Additional Considerations

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 and resource capacity, encryption keys, and other information and services needed to use Google Cloud Backup and DR Service 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.[12] [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.[13] [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.

2.5.2 Compliance Assessment

Cohasset upholds that the functionality of Google Cloud Backup and DR Service meets the requirement in SEC Rules 17a-4(f)(2)(v)(A) and 18a-6(f)(2)(v)(A) by retaining a persistent duplicate copy of the records, when the considerations described in Section 2.5.4 are satisfied.

2.5.3 Google Cloud Backup and DR Service Capabilities

- For compliance with paragraph (A), to maintain a redundant set of records, each backup vault is configured with a default storage location type which determines the replication services available for backups added to the backup vault.
  - Backups added to the backup vault use this default storage location type unless specified otherwise.
  - The regional location of the backup vault is permanent once it's assigned; therefore, it cannot be changed.

12 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66421.

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

- Currently, the only storage location type is regional, which provides redundancy across multiple availability zones within the designated region, in addition to redundancy across multiple disks, power, and network failure domains.
- The redundancy feature replicates both the backup contents and metadata, including retention controls.

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 Backup and DR Service and permit access to the redundant records.

2.6 Audit System

2.6.1 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.

2.6.2 Compliance Assessment

Cohasset asserts that Google Cloud Backup and DR Service supports the regulated entity's efforts to meet this SEC audit system requirement.

2.6.3 Google Cloud Backup and DR Service Capabilities

The regulated entity is responsible for an audit system, and compliance is supported by Google Cloud Backup and DR Service.

- For each Backup, Google Cloud Backup and DR Service stores a unique Global Identifier and system-generated creation timestamp. These attributes (a) are immutable, (b) uniquely identify each record, (c) chronologically account for each record, and (d) are retained for the same time period as the record.
  - The Global Identifier is comprised of (a) the backup vault name, which is unique within the specified Google Cloud region, (b) a data source name, which is unique within the specified backup vault, (c) a backup name, which is unique within the data source, and (d) a creation timestamp.

- Each backup (i.e., point-in-time archival copy of the original source) is immutably stored over its lifespan; therefore, no changes are allowed once the backup is finalized, and no changes are allowed to the collection of records and record metadata stored as the backup's content.
- In addition to the immutable backup metadata, Cloud Audit Logging can be enabled to log backup operations in GCP; activities include administrative activity, data access, system event and policy denied audit logs. Included in the logs are configured and modifying retention controls, such as the minimum enforced retention period and retention expiration date.
  - Each audited event tracks the user, action, timestamp and status (success or failure).
  - Audit logs can be viewed and searched directly within Google Cloud Console via a Logs Explorer page.
  - From the Logs Explorer the audit logs can be downloaded to JSON or CSV and may be ingested into external applications such as security information and event management tools.

2.6.4 Additional Considerations

The regulated entity is responsible for maintaining an audit system for inputting records and changes made to the records. In addition to relying on the immutable metadata, the regulated entity may utilize Cloud Audit Logging, with an appropriate retention period set or may copy the audit events to an external security information and event management system and keeping the audit events for the required retention period.

In addition, the regulated entity is responsible for: (a) authorizing user privileges, and (b) providing requested information to the regulator, in the requested format.

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

This section contains a summary assessment of the functionality of Google Cloud Backup and DR Service, as described in Section 1.3, *Google Cloud Backup and DR Service 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.*[14] [emphasis added]

In Section 2 of this report, Cohasset assesses Google Cloud Backup and DR Service, with backup vaults configured with a minimum enforced retention period, a highly restrictive configuration that assures the storage solution applies integrated controls to (a) protect immutability of the record content and certain system metadata and (b) prevent deletion over the applied retention period.

In the following table, Cohasset correlates specific *principles-based* CFTC requirements for electronic records with the functionality of Google Cloud Backup and DR Service, with backup vaults configured with a minimum enforced retention period. The first column enumerates the CFTC regulation. The second column provides Cohasset's analysis and opinion regarding the ability of Google Cloud Backup and DR Service to meet these requirements.

[14] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.

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[15] with time-based retention periods, are met by the functionality of Google Cloud Backup and DR Service, with the backup vaults configured with a minimum enforced retention period. The functionality that supports retention, authenticity and reliability of electronic records is described in the following sections of this report: ● 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 2.6, *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 Backup and DR Service retains immutable metadata (e.g., unique identifier that is systemically generated and stored for each backup). Additionally, metadata related to each record is stored in the backup, together with the archival copy of the records. Further, the audit logs for Google Cloud Backup and DR Service track audit events and provide options for exporting the audit events for retention in a separate system. For additional information, see Section 2.6, *Audit System*.
(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 Backup and DR Service capabilities to retain a persistent duplicate copy of the records and associated system metadata, as described in Section 2.5, *Record Redundancy*, 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*.

[15] 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)**
(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 Backup and DR Service 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, *Audit System*

4 • Conclusions

Cohasset assessed the functionality of Google Cloud Backup and DR Service[16] in comparison to the electronic recordkeeping system requirements set forth in SEC Rules 17a-4(f)(2) and 18a-6(e)(2) and described audit system features that support the regulated entity as it meets the requirements of SEC Rules 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii).

Cohasset determined that Google Cloud Backup and DR Service, when properly configured, has the following functionality, which meets the regulatory requirements:

- Retain backups and immutable backup metadata in non-rewriteable, non-erasable format for time-based retention periods when the backup is stored in a backup vault and a minimum enforced retention period is configured. Each backup retains an immutable collection of records and record metadata.
- Allow the retention expiration date to be extended for select backups to effectuate a legal hold for subpoenas, litigation, government investigations, external audits, and other similar circumstances.
- Prohibit deletion of a backup and its immutable metadata until its retention expiration date has expired.
- Verify the accuracy of the process for storing and retaining records, using Google Cloud Backup and DR Service validation processes.
- Provide authorized users with the capacity and tools to (a) search for a backup, and (b) recover a full backup (thus also enabling access to list backup contents and to copy specific content).
- Store compliant redundant copies of backup data and provides for the recovery of the backup data from the redundant copies.
- Support the regulated entity's obligation to retain an audit system for non-rewriteable, non-erasable records.

Accordingly, Cohasset concludes that Google Cloud Backup and DR Service, 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 audit system requirements in SEC Rules 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii). In addition, the assessed capabilities meet the principles-based electronic records requirements of CFTC Rule 1.31(c)-(d).

[16] See Section 1.3, *Google Cloud Backup and DR Service 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[17] 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.*[18] [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.*[19] [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.

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

[18] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66428.

[19] 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.*[20] [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.*[21] [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."*[22] [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****[23] [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).

---

20 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.
21 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.
22 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66418.
23 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.*[24] [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.*[25] [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.*[26] [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 Backup and DR Service 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).[27]

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.*

---

24 2003 Interpretative Release, 68 FR 25282.

25 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).

26 2003 Interpretative Release, 68 FR 25283.

27 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.*[28] [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 Backup and DR Service in relation to each requirement, see Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*.

[28] 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 agreed to in the Traditional Undertaking. Rather, it means that the third party undertakes to provide to the Commission

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]

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.[29] [emphasis added]

B.2 Google Undertaking Process

- To obtain an Alternative Undertaking for Google Cloud Backup and DR Service, 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 relieve 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, (d) maintaining technology, encryption keys and privileges to access Google Cloud Backup and DR Service, and (e) 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.

[29] 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.