Cohasset Associates

Google Workspace™

COMPLIANCE ASSESSMENT

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

Abstract

Google Workspace™ is a global, browser-based suite of productivity and collaboration services available on the Google Cloud Platform (GCP). Google leverages the capabilities of AODocs Compliance Archive by Altirnao, Inc., an advanced content management service that is tightly integrated with Google Workspace and Google Cloud Storage (GCS), to meet securities industry requirements for preserving electronic records in non-rewriteable, non-erasable format for applied retention periods and legal holds.

Additionally, Google offers its Digital Communications Governance and Archiving (**DCGA**) **Export Service** and Domain Wide Takeout (**DWT**) **Export Service.** Both services are designed to capture communications-based records for automated export to third-party DCGA platforms.

In this report, Cohasset Associates, Inc. (Cohasset) assesses the functionality of Google Workspace (see Section 1.3, *Workspace 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 Workspace with AODocs Compliance Archive, has functionality that meets the electronic recordkeeping system requirements outlined above. Additionally, the Google DCGA Export Service and DWT Export Service have functionality that supports the regulated entity in its compliance with SEC Rules specific to digital communications.

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.

September 2025

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

+1.312.527.1550 | Visit Cohasset website

Table of Contents

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 Workspace 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 Google Workspace with AODocs Compliance Archive for 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]

---

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.

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]

1.1.3 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 4, *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*.

1.1.4 Digital Communications Requirements

Regulated entities must comply with stringent regulatory mandates for required digital communications and certain recordings of oral conversations, including, but not limited to (a) retaining required communication artifacts for the mandated retention period, (b) implementing monitoring and supervisory review processes, and (c) retaining required digital communication artifacts in a format and media that complies with the electronic recordkeeping system requirements; see Sections 1.1.1, 1.1.2 and 1.1.3, above.

For additional information, refer to Section 3.1, *Overview of the Regulatory Requirements for Digital Communications and Oral Conversations*, and Appendix B, *Overview of Relevant Requirements for Digital Communications and Oral Conversations,* for excerpts of these regulations.

1.2 Purpose and Approach

To obtain an independent and objective assessment of the compliance capabilities of Google Workspace (Workspace) 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 Workspace, 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 Google Workspace with AODocs Compliance Archive for 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 Google Workspace with AODocs Compliance Archive for Compliance with SEC Rules 17a-4(f) and 18a-6(e)* and Section 3, *Assessment of Google Compliance Archiving Support for Digital Communications and Oral Conversations;*

- Associate the principles-based requirements of CFTC Rule 1.31(c)-(d) with the assessed functionality of Workspace; see Section 4, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d);*
- Assess the functionality of Google's Digital Communications Governance and Archiving (DCGA) Export Service and Domain Wide Takeout (DWT) Export Service to support regulated entities in meeting compliance requirements for digital communications and oral conversations; 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 Workspace and its functionality, other Google products or services, AODocs, or other Altirnao 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, (e) materials provided by Google or Altirnao, and (f) related materials 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 Workspace Overview and Assessment Scope

1.3.1 Workspace Overview

Google Workspace™ (Workspace) is a global, browser-based suite of productivity and collaboration services available on the Google Cloud Platform (GCP).

To meet securities industry requirements for preserving electronic records[4], three Workspace-specific compliance feature sets are offered, as enumerated below and summarized in Figure 1.

Google Workspace Services	Google Workspace with AODocs *Compliance Archive*	Google *DCGA Export Service*	Google *DWT Export Service*
Native files created in Google Drive, including Google Docs, Sheets, and Slides	✓		
Non-native files in Google Drive	✓		
Gmail		✓	
Google Calendar		✓	
Google Chat		✓	
Google Meet		Future support for DCGA is planned	✓

Figure 1: Compliance Feature Sets available for Google Workspace

[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 *record*, in addition to specific terms, e.g., data, file, object, digital content, or version, to recognize that the content may be required for regulatory compliance.

1. **Google Workspace with AODocs Compliance Archive** is used to archive, retain and manage Google Drive content (native and non-native) in non-rewriteable, non-erasable format for applied retention periods and legal holds.
2. The **Google DCGA Export Service** is used to automate the export of Gmail, Chat, and Calendar communication artifacts to third-party Digital Communications Governance and Archiving (DCGA) platforms.
3. The **Google Domain Wide Takeout (DWT) Export Service** enables automated export of Google Meet communication artifacts to third-party Digital Communications Governance and Archiving (DCGA) platforms.

An overview of each of these compliance feature sets is presented in the following subsections, and the scope of this assessment is presented in Section 1.3.2, *Assessment Scope*.

1.3.1.1 Google Workspace with AODocs Compliance Archive

Google leverages the capabilities of AODocs by Altirnao, Inc. Built natively on GCP, AODocs and the AODocs Compliance Archive model are tightly integrated with both Google Workspace and Google Cloud Storage (GCS).

- AODocs operates as a Google Workspace-integrated Drive application, with the associated libraries residing in the dedicated My Drive belonging to the AODocs service account.
- The AODocs Compliance Archive model assures that integrated controls are applied to records stored in GCS, which prevents record modification, overwrite and deletion until the applied retention period is expired and any legal holds are released.

Google Workspace with AODocs Compliance Archive is comprised of three main environments that reside on GCP. The logical storage architecture is depicted in Figure 2.

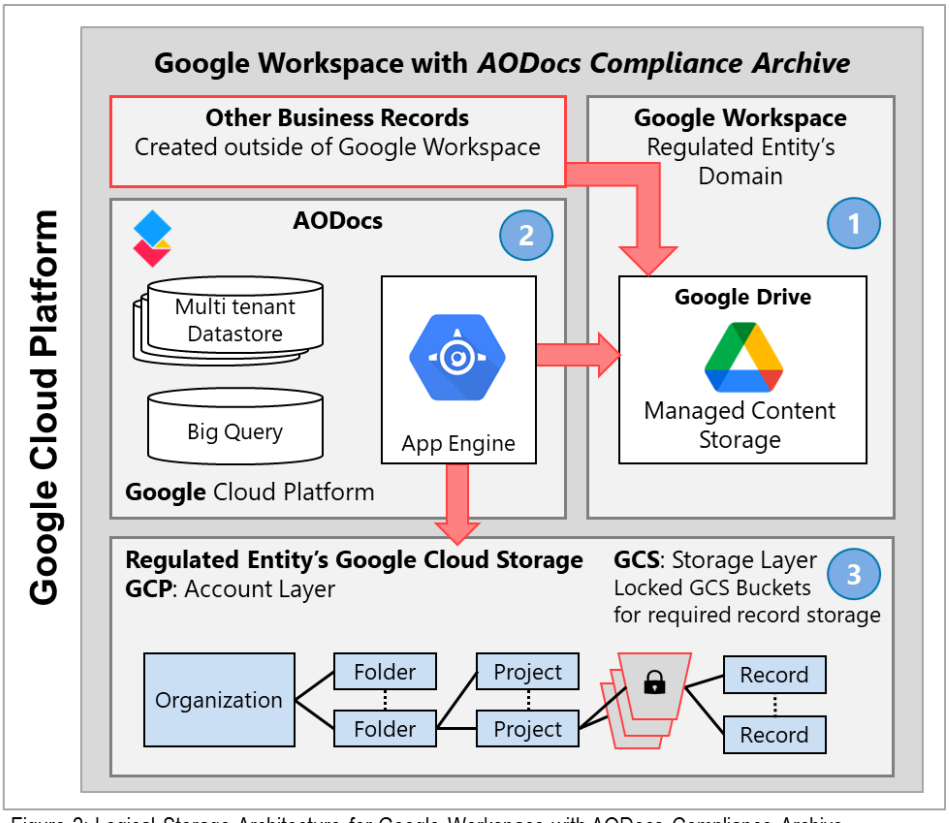

Figure 2: Logical Storage Architecture for Google Workspace with AODocs Compliance Archive

1. **Google Workspace** authenticates users, provides collaboration, and stores working copies of native and non-native content in the dedicated My Drive belonging to the AODocs service account.

- **Native**[5] **content** created in Google Docs, Sheets, and Slides is included for compliance with the Rules, whereas other native formats, such as Forms, are excluded.
- **Non-Native**[6] **content** uploaded to Google Drive, such as PDFs, images and video, is included for compliance with the Rules.

2. Altirnao's multi-tenant AODocs Compliance Archive components include: (a) the App Engine, an application server that hosts AODocs content management services, (b) the Multi-Tenant Datastore, a data repository where AODocs retains properties (i.e., metadata for managed content), as well as audit log data, and (c) a BigQuery data warehouse, used to retain replicated audit log data as well as user-defined reporting data.
3. The **regulated entity's GCS** account serves as the compliant *storage subsystem*. Information resources within the Account are organized into Folders and Projects, which utilize GCS Buckets with locked Bucket Retention Policies to store required records. When managed content in Drive is *finalized* (i.e., declared a record) via a manual action or workflow transition, the record is transferred to a locked GCS Bucket and immutably stored for the duration of the applied retention period, as defined by a GCS Bucket Retention Policy.

See Section 2, *Assessment of Google Workspace with AODocs Compliance Archive for Compliance with SEC Rules 17a-4(f) and 18a-6(e),* for additional information.

1.3.1.2 Google DCGA Export Service

As part of Google Workspace, the Google **DCGA Export Service** is designed to support regulated entities in meeting financial industry requirements for preserving, monitoring, supervising, and managing required digital communications.

The logical process flow is illustrated in Figure 3 and described as follows:

1. Monitored users who are subject to financial industry requirements for communications are identified by Organizational Unit (OU) or Group for the following communication services.
   - Gmail messages, including outbound and inbound email messages and Google Calendar invitations sent to meeting participants.
   - Google Chat messages, including both (a) direct messages (i.e., DMs) for one-to-one and one-to-many small

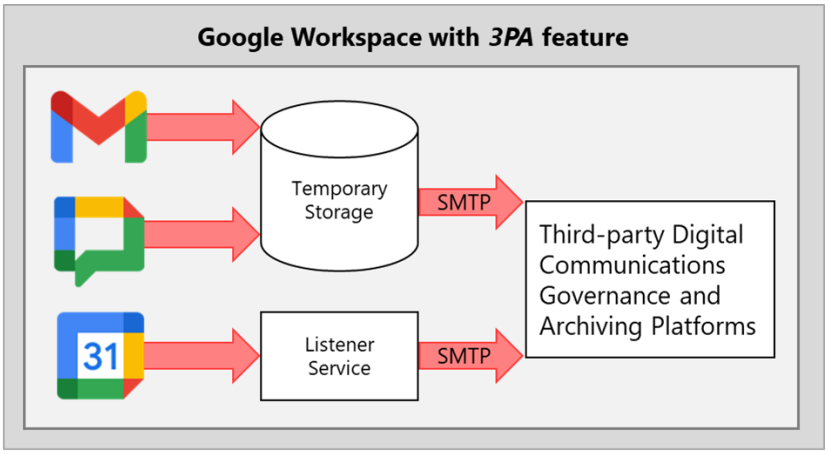

Figure 3: Logical process flow

[5] Native content is created in Google Workspace applications such as Docs, Sheets, or Slides and are stored in a proprietary data file format on Google Drive.

[6] Non-native files are created outside of the Google Workspace environment, via third-party applications such as Microsoft Office or Adobe, and uploaded to Google Drive for storage.

group communications and (b) persistent chat spaces for posting team-based communications. Note: Google In-Meeting Chat messages are excluded from the DCGA Export Service.

- Google Calendar events, e.g., event name, date, time, location, description, links to attachments, and reminders associated with those events.

2. Gmail and Google Chat Messages for monitored users are written to a temporary message queue. Then, using SMTP, the messages are exported to the third-party Digital Communications Governance and Archiving Platform, as setup by the Administrator.
3. For Calendar events involving a monitored user, the Listener Service generates an email message with an iCalendar file (ICS) attachment, which is exported using SMTP to the third Digital Communications Governance and Archiving Platform, as setup by the Administrator.

See Section 3, *Assessment of Google Compliance Archiving Support for Digital Communications and Oral Conversations,* for additional information on the Google DCGA Export Service.

1.3.1.3 Google DWT Export Service

As part of Google Workspace, the Google **DWT Export Service** is designed to support regulated entities in meeting financial industry requirements for preserving, monitoring, supervising, and managing required oral conversations recorded by Google Meet, as well as related transcripts and meeting attendance information.

The logical process flow is illustrated in Figure 4 and described as follows:

1. Monitored meeting hosts, who are identified as subject to financial industry requirements for recording oral conversations are identified by Domain, OU or Group, for the capture of Meet artifacts, which include meet recordings, transcripts associated with the Meet recordings, and meeting attendance.
2. Meet artifacts for monitored users are stored in Google Drive storage for the meeting hosts.
3. DWT exports a copy of the Meet artifacts to a temporary GCS Storage Bucket with a locked Retention Policy.

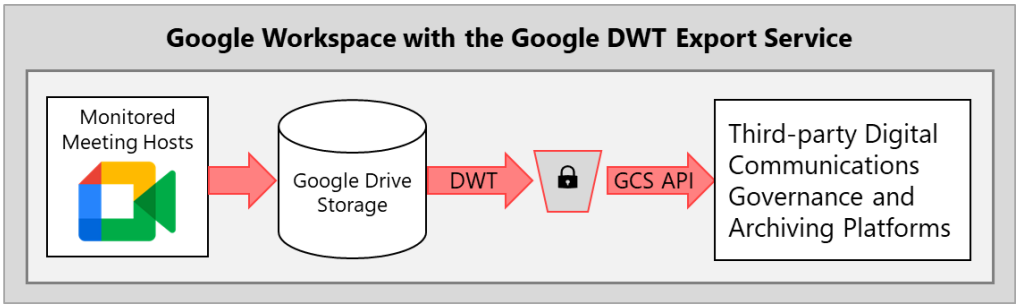

Figure 4: DWT Logical process flow

4. Then, using a GCS API, the Meet artifacts are exported to a third-party Digital Communications Governance and Archiving Platform, as setup by the Administrator.

Notes: Google In-Meeting Chat messages are excluded from the DWT Export Service. Additionally, Meeting hosts and co-hosts can override and thereby block the automated capture of Meet artifacts for an explicit meeting.

See Section 3, *Assessment of Google Compliance Archiving Support for Digital Communications and Oral Conversations,* for additional information on the Google DWT Export Service.

1.3.2 Assessment Scope

The scope of **Section 2, *Assessment of Google Workspace with AODocs for Compliance with SEC Rules 17a 4(f) and 18a 6(e)*,** is focused on the compliance-related capabilities of Google[7] with AODocs Compliance Archive, operating under the following configurations and deployments:

- A Google Workspace domain or organizational unit, owned by the regulated entity, must have (a) a Google Workspace licensing option that provides access to the *Domain Wide Takeout* feature and (b) an AODocs Application Platform license subscription, with at least one AODocs instance configured.
  - The AODocs Retention Application, including the AODocs Compliance Archive with Immutable Storage module, must be acquired as a separate licensing subscription for the AODocs environment to be *capable* of leveraging the GCS *Bucket Lock* feature for immutable retention of records.
- A Google Cloud Platform (GCP) account and GCS storage subsystem, owned by the regulated entity, must be established, with the following GCP configurations:
  - A GCP Project must be created and an AODocs service account with appropriate GCS ownership permissions, must be added. This allows the AODocs Retention Application to (a) automatically create Buckets, with the *Bucket Lock* feature enabled and (b) store records within those Buckets.
  - A *Lien* should be set at the GCP Project-level that is inherited by the Buckets, to prohibit inadvertent Bucket deletion in the event a GCP Project is removed from the Account layer of GCP.

The scope of **Section 3, *Assessment of Google Compliance Archiving Support for Digital Communications and Oral Conversations*,** is focused on assessing the Google DCGA Export Service and the Google DWT Export Service, as well as other capabilities that support compliance archiving of digital communications and recordings of oral conversations, when operating under the following configurations and deployments:

- For Google DCGA Export Service:
  - A Google Workspace domain or organization unit, owned by the regulated entity, must have a Google Workspace licensing option that provides access to the Google DCGA Export Service.
- For Google DWT Export Service:
  - A Google Workspace domain or organization unit, owned by the regulated entity, must have a Google Workspace licensing option that provides access to the Google DWT Export Service.
  - A Google Cloud Platform (GCP) account and GCS storage subsystem, owned by the regulated entity, must be established, with the following GCP configurations:
    - A GCP Project must be created to allow for the creation of a Bucket, with the *Bucket Lock* feature enabled, to be used by the DWT Export Service to temporarily store Meet artifacts prior to export. Note: A *Lien* should be set at the GCP Project-level that is inherited by the Bucket, to prohibit inadvertent Bucket deletion in the event a GCP Project is removed from the Account layer of GCP

[7] Google functionality includes Google Drive native content (i.e., Google Docs, Sheets and Slides) and non-native content (i.e., PDFs, images, video and other files uploaded to Google Drive), Google Cloud Storage, and other GCP features.

- Additionally, the regulated entity designates monitored users subject to books and records requirements and configures the export process to utilize a third-party archiving solution to receive and store the digital communications records. Further, the third-party archiving solutions must have compliance capabilities that are properly configured and applied to records for compliance with the requirements of the Rules.

NOTES:

- Workspace with AODocs Compliance Archive leverages the GCS *Bucket Lock* feature to ensure immutable storage of electronic records. Therefore, this assessment excludes the GCS *Object Retention Lock* feature.
- For digital communications, this assessment does not address the capabilities of the third-party archiving solution; instead, this report assesses Google capabilities, such as the Google DCGA and DWT Export Services that support compliance archiving of digital communications and oral conversations.
- Additionally, this Compliance Assessment Report excludes:
  - Google services not included in Section 1.3, e.g., Google Forms, Google Drawings, Google Apps Script, Google Voice, Google Sites, Google Keep (Notebook), Google Tasks, Google Vids, Google Gemini and Google Vault.
  - Files stored on Google Shared Drives or in user My Drives. (This assessment only includes files stored in the dedicated My Drive belonging to the AODocs service account.)
  - Google In-Meeting Chat, which must be disabled, if the contents are considered required records.
  - Live Stream Meetings, Meet Calls (formerly Duo) and Meet Legacy Calls are out of scope for this assessment.
  - Other applications that are available through the Google Workspace Marketplace.
  - Software-as-a-Service solutions, other than AODocs that are not managed by Google.

2 • Assessment of Google Workspace with AODocs Compliance Archive for Compliance with SEC Rules 17a-4(f) and 18a-6(e)

This section presents Cohasset's assessment of the functionality of Google Workspace with AODocs Compliance Archive, 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 Workspace
- ***Workspace 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 Workspace, as described in Section 1.3, *Workspace 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.*[8] [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.*[9] [emphasis added]

2.1.2 Compliance Assessment

In this report, Cohasset has not assessed Workspace 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 Workspace, with the features and controls described in Sections 2.2 through 2.9 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.

> *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*

8 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.

9 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66418.

> *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.*[10] [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.*[11] [emphasis added]

2.2.2 Compliance Assessment

It is Cohasset's opinion that the functionality of Google[12] with AODocs Compliance Archive meets this SEC requirement to retain records in non-rewriteable, non-erasable format for the applied time-based[13] retention periods and any applied legal hold, 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 Workspace Capabilities

This section describes the functionality of Google Workspace with AODocs Compliance Archive 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 Definitions

The following terms are defined to aid in understanding the capabilities of AODocs Compliance Archive, an advanced content management service that is tightly integrated with Google Workspace and Google Cloud Storage (GCS) for compliance with SEC Rules.

---

10 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66419.

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

12 Google functionality includes (a) Google Workspace to authenticate users and provide collaboration, (b) Google Drive to store working copies of native content (i.e., Google Docs, Sheets and Slides) and non-native content (i.e., other Google Drive files, such as PDFs, images and video), (c) Google Cloud Storage for final records, and (d) other Google services.

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

Term	Definition
AODocument, a.k.a. AODocs Document	A logical management document comprised of (1) a set of properties (metadata), (2) a workflow state, if applicable, and (3) links to Attached Files and/or to other AODocuments. Any number of artifacts (zero to many) can be attached to an AODocument. Each AODocument also contains a title, description, unique URL, and document identifier.
Attached Files / Attachments	A Google Drive file that is attached to an AODocument. Attached Files, although managed by AODocs, remain stored in the regulated entity's Google Drive and are copied to GCS for SEC-compliant storage. Any format (native or non-native) supported by Google Drive is supported as an attachment to an AODocument. ● Native files are created via Google Workspace applications such as Docs, Sheets, or Slides and are stored in a proprietary format on Google Drive and in Microsoft Office format on GCS. ● Non-native files are created outside of the Google Workspace environment, via third-party applications such as Microsoft Office or Adobe, and uploaded to Google Drive for storage. Non-native files are retained in their original format on both Google Drive and in GCS.
Document Class	A set of configuration parameters that define a type of AODocument, such as an invoice, purchase order, or contract. Each Document Class has its own list of defined or expected properties (i.e., an invoice may have an amount due, a due date, and an accounting code), security permissions, reporting capabilities, and can be assigned its own workflow. Folders can be associated with a Document Class and used to further organize and manage the AODocuments.
Document Library, a.k.a. AODocs Document Library	A logical container used by AODocs to manage/organize AODocuments. For example, an HR Library may be used to store AODocuments related to personnel matters. There are three types of Document Libraries available for use by the regulated entity, each offering progressively more granular controls: (1) Team Folders Libraries, (2) Secured Folders Libraries, and (3) Document Management Libraries.
Properties	Also referred to as metadata, a property is an element of an AODocument or Retention Document. There are two types of properties: (1) system properties, such as creation date, last update date, document creator, etc. and (2) custom properties, as defined for the type of Document Class, such as contract expiration date or invoice amount.
GCS-stored Record	A required record that is immutably retained within a GCS Bucket according to the assigned Retention Schedule. A GCS-stored record is comprised of: ● A point-in-time copy of a finalized AODocument (i.e., one that has been declared a record). ● A point-in-time snapshot of each Google Drive file that is attached to the finalized AODocument, including associated system properties for each. ● The GCS Global Identifier, along with the GCS storage timestamp.
Retention Document	A unique type of AODocument, used exclusively by AODocs Compliance Archive to retain the relationship mapping between (a) original Attached Files in Google Drive, (b) original AODocument, and (c) GCS-stored records.
Retention Class	A unique type of Document Class used within the Retention Library. Each Retention Class corresponds to a single GCS Bucket (i.e., there is a 1:1 relationship between an AODocs Retention Class and GCS Bucket) and has a pre-defined set of retention properties.
Retention Library	A special type of AODocument Library used to manage and organize Retention Documents, according to their Retention Classes. The Retention Library, with its stored Retention Documents, serves as the primary index of all GCS-stored records.
Retention Schedules	Retention policies, or rulesets that define the Retention Time and retention controls enforced when the Retention Schedule is applied to a finalized AODocument.

Term	Definition
[AODocs] Event	A property used to determine how the start of the retention period is determined. For required records, the 'triggering event' occurs when an AODocument and its attachments are finalized, and a snapshot is immutably stored in a GCS Bucket. Note: This property name should not be confused with the more traditional records management term event-based[14] retention.
[AODocs] Event Date	A date that indicates the start of the retention period, i.e., the date of the 'triggering event'. Note: This property name should not be confused with the more traditional records management term event-based retention date.
Lifecycle State	A flag set by AODocs to either *active* (i.e., prior to the start of an assigned Retention Time) or *control* (i.e., controlled by a Retention Schedule) with a snapshot immutably retained in GCS.

2.2.3.2 Overview

- To meet the non-rewriteable, non-erasable record format requirements of the SEC Rules, the regulated entity's Workspace Accounts must be properly configured for use with AODocs Compliance Archive, which enables the use of integrated GCS *Bucket Lock* controls.
- When native[15] and non-native[16] files, stored in Google Workspace, are determined to be business records (i.e., collaboration is complete), the managing AODocument must be *finalized* within the AODocs environment, via manual action or automatic workflow transition.
- Retention controls are applied to each finalized record as follows:
  - Write permissions are removed and retention is applied to the **AODocument**, based upon a pre-defined Compliance Archive Retention Schedule. A *Target Destruction Date* is calculated and retained as a property of the AODocument.
  - Write permissions are removed and an *Archive in Progress* Drive label is applied to each Attached File in Drive that is managed by the AODocument.
  - Google Domain Wide Takeout (DWT), a recurring data export process, identifies all finalized and/or labeled record components and exports a point-in-time snapshot of (a) each finalized AODocument and (b) the top-level rendition of each Attached File, including associated system properties for each. These elements, collectively, represent the GCS-stored record.
  - The elements of the record are written to a GCS Bucket with a locked retention policy that matches the AODocument's assigned retention.

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

[15] For purposes of this assessment, native files only include Google Docs, Sheets and Slides.

[16] For purposes of this assessment, non-native files includes Google Drive content created outside of the Google Workspace environment, such as PDFs, images and video.

- A Retention Document is automatically created in the AODocs Retention Library to retain the relationship mapping between (a) the source Attached Files in Google Drive, (b) the source AODocument in the AODocument Library, and (c) the immutable GCS-stored record.

► The following table summarizes the highly-restrictive retention controls applied to GCS-stored records, which are written to a locked GCS Bucket. See the subsections following this *Overview*, for information on configuring the retention features and the resulting integrated controls.

	Locked GCS Bucket with highly-restrictive integrated retention controls
Protecting record content and immutable system metadata	• By design, a GCS-stored record and its associated system metadata cannot be modified or overwritten for the duration of the applied retention period. • Renaming GCS-stored records is prohibited. • Renaming GCS Buckets is prohibited.
Restricting changes to retention controls	• Retention, once applied to a GCS-stored record, cannot be shortened, extended or deleted. Note: If the retention period must be extended, a record may be copied to a different GCS Bucket that has a Bucket Retention Policy with a longer retention duration. The copied record will inherit retention from the target Bucket. • See Section 2.2.3.4, *Record Definition and Controls*.
Applying and removing legal holds	• A legal hold may be applied to a finalized record which prevents deletion of the GCS-stored record until the hold is removed. • See Section 2.2.3.5, *Legal Holds (Temporary Holds)*.
Restricting deletion of Google Accounts, GCS Buckets and records	• Finalized source AODocuments and Retention Documents are eligible for deletion from AODocs Document Library and Retention Library when the Target Destruction Date is in the past and any legal hold is removed. • Records in the GCS Bucket are eligible for deletion when the applied retention period has expired and any legal hold is removed. • See Section 2.2.3.6, *Deletion Controls.*

2.2.3.3 Retention-related Configurations

► For compliance with SEC Rules, retention-related configurations are required in both (1) the regulated entity's Google Cloud Platform GCS storage environment and (2) the regulated entity's Google Workspace domain, integrated with its AODocs environment. The following table describes these retention-related configurations; see Section 2.2.3.4, *Record Definition and Controls*, for details on the resulting integrated controls applied to GCS-stored records.

	Workspace with AODocs Compliance Archive – Retention-related Configurations
(1) Regulated Entity's Google Cloud Platform GCS Storage Environment	
GCP Project with Lien	• A GCP Project must be created and an AODocs service account with appropriate GCS ownership permissions, must be added. This allows the AODocs Retention Application to (a) automatically create Buckets, with the *Bucket Lock* feature enabled and (b) store records within those Buckets. • A Lien should be set at the GCP Project-level that is inherited by the Buckets, to prohibit inadvertent Bucket deletion in the event a GCP Project is removed from the Account layer of GCP. Note: Cohasset recommends that the creation of Project-level Liens be automated within the regulated entity's GCP environment, which provides enforcement of governance policies by preventing administrators with

	Workspace with AODocs Compliance Archive – Retention-related Configurations
	special privileges from inadvertently removing Project-level Liens and associated storage Buckets that may contain unexpired required records.
GCS Temporary Storage Bucket	● A GCS **Temporary Storage Bucket** is leveraged by the AODocs Compliance Archive to temporarily hold records prior to being copied to other GCS Buckets for long-term immutable retention. The Temporary Storage Bucket must be configured as follows: ○ A retention duration (i.e., 30 days is recommended) is applied as the Bucket's retention policy. ○ The Bucket retention policy is *locked* (lock status set to *true,* a.k.a., a locked GCS Bucket) to assure the Bucket's retention duration cannot be shortened or removed. ○ Object versioning is disabled for the Bucket. ○ The Bucket is linked to the AODocs Retention Application. ○ A Google Cloud Object Storage Lifecycle deletion rule is set to a value equal to the Bucket retention policy to ensure all temporary records are removed once past their retention period.
(2) Regulated Entity's Google Workspace Domain, integrated with its AODocs Environment	
Retention Library	● An AODocs Retention Library must be configured to store Retention Documents, which are used as the primary index for locating GCS-stored records. Optionally, a duplicate Retention Library may be configured to retain a persistent duplicate copy of the index.
Retention Audit Logs Library	● A Retention Audit Logs Library, with a dedicated Retention Logs Class, must also be configured to track both human-originated and application-originated exceptions that might occur during the lifecycle of retained records, as well as key lifecycle activities.
Retention Schedules	● Retention Schedules must be created in the AODocs environment, as described in the following sub-bullets, to define the retention controls enforced when the Retention Schedule is applied to a record. ○ Retention Schedules are created within the AODocs Retention Application, either (a) manually by authorized AODocs super administrators or (b) automatically via uploading a CSV (comma-separated value) file. ○ The following retention properties must be set for a Retention Schedule to assure the application of compliant retention controls: ▪ Compliance Archive: This flag must be set to *Yes* to identify that the Retention Schedule will be used for compliance with SEC Rules (herein after referred to as a Compliance Archive Retention Schedule). ▪ Retention Time: This property specifies the number of years past the AODocs Event timestamp that a GCS-stored record must be immutably retained in a locked GCS Bucket. If set to a value of -1, retention is permanent within AODocs and 100 years in the GCS Bucket. ○ The Compliance Archive Retention Schedule must be assigned to one or more of the following: (a) an AODocs Document Library, (b) a folder, or (c) a sub-folder within an AODocs Document Library. Once assigned, it will be used to calculate retention for records when they are finalized. Note: Multiple *Compliance Archive Retention Schedules* may be applicable to a single record; in this case, the longest associated retention period is used when writing the GCS-stored record. ● When a Compliance Archive Retention Schedule is created, the AODocs Retention Application automatically triggers the following actions: ○ In GCS, a Bucket is created and (a) the Retention Time defined in the AODocs Compliance Archive Retention Schedule is applied as the GCS Bucket's retention policy, (b) the GCS Bucket retention policy is locked (lock status set to *true;* a.k.a., a locked GCS Bucket), to assure the retention duration cannot be shortened or removed on the GCS Bucket, and (c) object versioning is disabled for the GCS Bucket. Note: Only one retention period is allowed per GCS Bucket. ○ In the AODocs Retention Library, a Retention Class is created that corresponds to the new GCS Bucket. By default, the AODocs Retention Class is automatically configured with a pre-defined set of retention properties, used for cross referencing the records retained in GCS Buckets to the source AODocument (stored in AODocs) and Attached Files (stored in Google Drive).

	Workspace with AODocs Compliance Archive – Retention-related Configurations
Document Libraries	● AODocs Document Libraries must have a Compliance Archive Retention Schedule assigned to the Document Library, folder or sub-folder to enable the application of retention controls when an AODocument is finalized, within the container. Before a Compliance Archive Retention Schedule can be assigned, however: ○ The Document Library must be configured to support the receipt of dynamic values for the Retention ID property (i.e., an AODocument-level property). ○ Each Document Class defined for the Document Library must also be configured to (a) allow documents to be organized into folders, (b) support the Compliance Archive Retention Schedule properties, and (c) support the following additional retention properties. ▪ **Life Cycle State:** A flag automatically set by AODocs to either *active* (i.e., prior to the start of an assigned Retention Time) or *control* (i.e., controlled by a Retention Schedule with a snapshot immutably retained in GCS). ▪ **Event Date:** The date when retention controls are triggered (i.e., the AODocument enters the control Lifecycle State and a snapshot is written to GCS). This value is filled automatically by AODocs with the snapshot timestamp. ▪ **Target Destruction Date:** The date when the record in GCS becomes eligible for destruction, as calculated by adding the retention period to the AODocs Event Date. ▪ **On Hold:** A Boolean flag used to suspend retention controls in cases where a legal hold requires indefinite retention.

2.2.3.4 Record Definition and Controls

- Three primary storage areas are leveraged for Google Workspace with AODocs Compliance Archive, as illustrated in Figure 5 and described as follows:

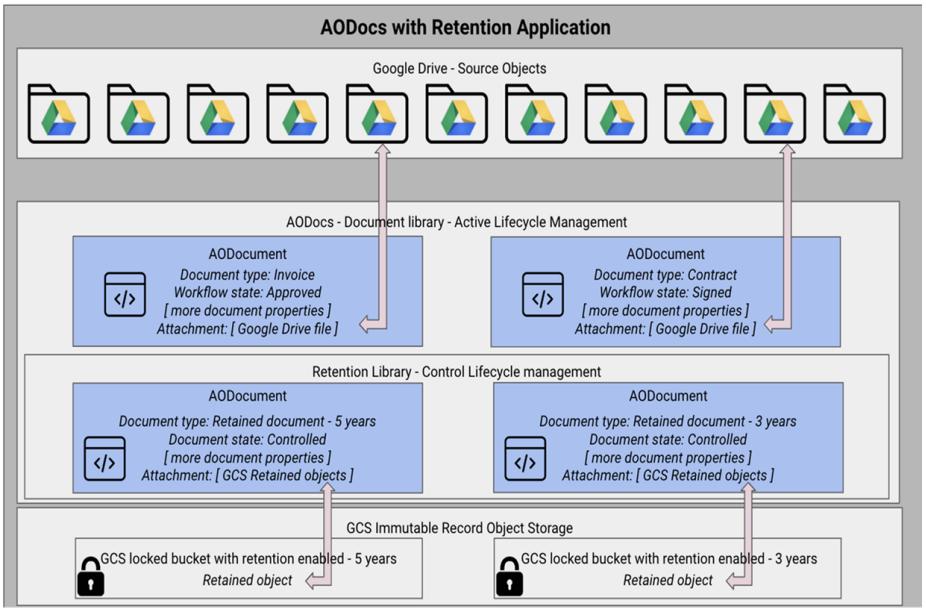

Figure 5: AODocs Data Organization

1. Collaboration is performed in Google Workspace, which uses a dedicated My Drive belonging to the AODocs service account to store working copies of native content (i.e., Docs, Sheets and Slides) and non-native files (e.g., scanned images, PDFs and other user uploaded files), as well as associated system metadata (e.g., last modification date).
2. AODocs Libraries retain system and custom properties to facilitate the *management* of Attached Files as well as GCS-stored records, which are immutably stored in locked GCS Buckets.

- **Document Libraries and Document Classes** manage AODocuments that are in an *active* lifecycle state. AODocuments consist of links to Google Drive Attached Files, as well as workflow comments, workflow status, and other defined custom properties.
- **Retention Library and Retention Classes** manage Retention Documents, which maintain relationship mapping (i.e., links) between the source Google Drive Attached Files, source AODocuments, and immutable GCS-stored records. The following system and custom properties (metadata) are retained in the Retention Document:
  - Unique ID, Retention Time, AODocs Event Date, Target Destruction Date, checksums, and legal hold flag.
  - Additional metadata for each Attached File from Google Drive includes title of document, version ID, creator, creation timestamp, last edit timestamp.

3. GCS Buckets with the *Bucket Lock* feature enabled (i.e., locked GCS Buckets), are used to immutably retain records with highly-restrictive integrated retention controls for compliance with the Rules. Each record within GCS is comprised of:
   - The complete content of the Attached Files (i.e., snapshot of the source Drive content).
   - The complete content of the finalized AODocument.
   - Immutable system metadata, which includes, but is not limited to: (1) a **GCS Global Identifier**, comprised of (i) the Bucket name, which is unique across the entire GCS namespace and (ii) a record name, which is unique within the Bucket; (2) the GCS storage timestamp; and (3) checksums.
   - Mutable metadata, which includes the GCS Temporary Hold flag (legal hold).

- When an AODocument is finalized, via a manual action or a workflow transition, Workspace with AODocs Compliance Archive performs the following:
  - The AODocument is assigned the following properties: (a) a *Pending Snapshot* property which prohibits further modifications to the AODocument by the regulated entity, (b) a Lifecycle State of *control*, (c) an AODocs Event Date set to the current system timestamp, (d) a Retention Time property, according to the longest retention period of any assigned *Archive Compliance Retention Schedules*, and (e) a calculated Target Destruction Date (AODocs Event Date plus Retention Time plus aggregation to the end of the quarter).
  - Google Drive files that are attached to the finalized AODocument are assigned a custom Google Drive Label of *Archive in Progress* and the sharing permissions of the Google Drive files are set to view-only, preventing further modification or deletion by the regulated entity.
    - The applied Google Drive Label of *Archive in Progress* can only be removed by a user with elevated privileges, such as the storage administrator.

  Note: Finalized AODocuments and attached Google Drive files remain in their source location, and the following process creates and writes the GCS-stored records.

- A Google *Domain Wide Takeout* export process runs at a pre-configured time each day and performs the following actions:
  - A **snapshot** is captured of the current *top-level rendition*[17] of Google Drive Attached Files with a custom Google Drive Label of *Archive in Progress*.
    - Collaborative *chats* that occur while editing a Google Workspace document are not captured as part of the snapshot.
    - Embedded comments (resolved and unresolved) within Google Workspace files are anchored to the appropriate sections of the snapshot.
    - Snapshots of native Google Workspace content (i.e., Docs, Sheets, Slides) are converted to Microsoft Office format prior to being written to GCS. Non-native files remain in their original format (e.g., DOC, XLS, PDF, TIF, JPG, MP4).
  - Snapshots, with associated system metadata, are bundled into a zip file and exported to the GCS Temporary Storage Bucket.
    - If errors are encountered during the export process, a failure report is generated for review and error correction by AODocs administrators.
- The AODocs Compliance Archive monitors the GCS Temporary Storage Bucket for new zip files. When detected, the following actions occur:
  - After verifying the integrity of the zip file and its contents, each snapshot is mapped to its corresponding AODocument to determine its assigned Retention Time.
  - The snapshot and its system metadata are copied from the GCS Temporary Storage Bucket to a long-term GCS Bucket with a locked retention policy that matches the record's assigned Retention Time. Note: A control operation is performed to ensure that each record object is copied into long-term GCS Buckets only once for immutable retention.
    - The *Archive in Progress* Google Drive Label is removed from the *source* Google Drive file to assure the zip file is not included again in the next *Compliance Takeout* export process. However, the source Google Drive file retains view-only permissions.
  - The AODocument's *Pending Snapshot* property is changed to *Final* and a snapshot of the AODocument is written to the long-term GCS Bucket and becomes the final element of the GCS-stored record.
  - A Retention Document is automatically created in the AODocs Retention Library to retain the relationship mapping between (a) the source Attached Files in Google Drive, (b) the source AODocument in the AODocs Document Library, and (c) the immutable GCS-stored record in a locked GCS Bucket.

[17] Google automatically maintains a detailed version history of native files (e.g., Docs, Sheets, Slides). Prior versions may be viewed and/or restored as the *top-level rendition* (i.e., current version) at any time. Additionally, versions of non-native files may be manually saved to Google Drive, allowing for prior versions to be viewed and/or restored as the *top-level rendition* as needed.

- The following table describes the highly-restrictive integrated retention controls applied to each GCS-stored record in a locked GCS Bucket.

	Locked GCS Bucket with highly-restrictive integrated retention controls
Protecting record content and immutable system metadata	● By design, a GCS-stored record and its associated system metadata cannot be modified or overwritten for the duration of the applied retention period. All attempts to modify or overwrite the content of a record or its immutable system metadata are rejected. ● Renaming records is prohibited. ● Renaming GCS Buckets is prohibited.
Restricting changes to retention controls	● A Compliance Archive Retention Schedule, once assigned to a Document Library, folder or sub-folder, cannot be removed if one or more records have been written to a GCS Bucket using the Retention Schedule. ● A GCS Bucket Retention Policy, once locked, cannot be modified or removed. ● Retention, once applied to a GCS-stored record, cannot be shortened, extended or deleted. Note: If the retention period must be extended, a record may be copied to a different GCS Bucket that has a Bucket Retention Policy with a longer retention duration. The copied record will inherit retention from the target Bucket.
Applying and removing legal holds	● A legal hold may be applied to a finalized record which prevents deletion of the GCS-stored record until the hold is removed. ● See Section 2.2.3.5, *Legal Holds (Temporary Holds).*
Restricting deletion of Google Accounts, GCS Buckets and records	● Finalized AODocuments, and Retention Documents are eligible for deletion from AODocs Document Library and Retention Library when the Target Destruction Date is in the past and any legal hold is removed. ● Records in the GCS Bucket are eligible for deletion when the applied retention period has expired and any legal hold is removed. ● Decommissioning of Google environments is not restricted, meaning the regulated entity's administrator may decommission: ○ Workspace domains or user accounts, including the AODocs service account. ○ GCS storage environment by deleting their GCP Account, removing non-automated Project-level Liens and then deleting Projects and Buckets. Note: Deleting non-automated Project-level Liens requires the ***resourcemanager.projects.updateLiens*** permission. Should the regulated entity's administrator have this permission and decommissions any of the above environments, it may result in the premature deletion of unexpired records. Therefore, Cohasset recommends the use of automated Project-level Liens within the regulated entity's environment to enforce governance policies; otherwise, procedural controls and monitoring are required to scrutinize privileged administrative actions which may result in the premature deletion of records. ● See Section 2.2.3.6, *Deletion Controls.*
Copying records	● A record may be *copied* to another GCS Bucket. ● When a record is copied to another GCS Bucket with a locked retention policy (a) the copy inherits retention controls from the target Bucket and (b) AODocs automatically creates a new Retention Document in the Retention Library to retain the relationship mapping to the copy. Therefore, records may be copied to extend the applied retention period.
Moving records	● A record in GCS cannot be *moved* to another GCS Bucket. ● An AODocument in the AODocs Document Library with a property of *Final* cannot be moved to a new Retention Class.

2.2.3.5 Legal Holds (Temporary 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.

- A legal hold may be applied to an AODocument once it has been finalized. Authorized AODocs users search Retention Documents (i.e., the Index for records stored in GCS) to identify finalized records subject to the hold. The *On Hold* property is then set to *Yes* for all identified Retention Documents, preventing the deletion of properties (metadata) for the identified record, even if past its retention period.
  - Additionally, by setting the *On Hold* property, the *Temporary Hold* flag is automatically set on the record stored in the GCS Bucket, to enforce continued immutability and prohibit both overwrite and deletion of identified records until the hold is removed.
- The *On Hold* property can be removed from Retention Documents when no longer required which automatically removes the corresponding *Temporary Hold* flag in GCS. Thereafter, immutability controls for the record are governed by the retention setting assigned to the record.

2.2.3.6 Deletion Controls

- The following table summarizes when records are eligible for deletion and allowed actions to delete records and storage locations.

	AODocs	***Drive***	***GCS***
Eligibility for Deletion	• AODocuments and Retention Documents are *eligible for deletion* from the AODocs environment when **both** of the following conditions are met: ○ The *Target Destruction Date* is in the past, and ○ The *On Hold* flag is removed.	• Attached Files (source Google Drive files attached to AODocuments) are eligible for deletion when the managing AODocuments has reached is retention commitment.	• Records in GCS Buckets are eligible for deletion when: ○ The Retention Expiration Time is in the past (i.e., the applied retention period has expired). ○ The Temporary Hold flag is removed.
Deletion of Eligible Records	• Within the AODocs environment, users with appropriate permission may manually initiate deletion of eligible AODocuments, attached source Google Drive files, and Retention Documents. • Deleted AODocuments, attached source Google Drive files, and Retention Documents are moved to Trash where they remain for a pre-configured wait time, allowing administrators to restore them if necessary. While in Trash, documents/folders are not visible on any library views. Once past the pre-configured wait time, documents are permanently deleted from AODocs and Google Drive.		• Records in GCS Buckets, including the GCS Temporary Storage Bucket that are eligible for deletion are automatically removed during a quarterly disposition process. Disposition review and approval processes may be configured by the regulated entity, if needed.

	AODocs	***Drive***	***GCS***
Deletion of storage units and environments (e.g., Buckets, Accounts)	• Super administrators or Retention Library administrators are not restricted from deleting the following: ○ The Retention Library and/or Retention Classes from the Retention Library, including all references to records stored in locked GCS Buckets. ○ The Retention Log Class. ○ A Retention Log document. • Should deletion occur, the action is logged in the AODocs audit log database (hosted in the Datastore and replicated to the BigQuery database), the super administrator is notified via email, and the items must be manually recovered by the administrator.	• The regulated entity's administrator may delete the Google Workspace domains or user accounts, including the AODocs service account. This deletion could result in the removal of attached Google Drive files. Should any of these account entities be inadvertently deleted, the environment must be manually recovered by the administrator.	• The regulated entity's administrator may delete their GCS storage environment by deleting their GCP Account, removing non-automated Project-level Liens (and then deleting Projects and Buckets with records that may not yet be eligible for deletion). Should any of these actions occur, the environment must be manually recovered by an administrator. Note: Deleting Project-level Liens requires the ***resourcemanager.projects.updateLiens*** permission. Should the regulated entity's administrator have this permission and decommissions any of the above environments, it may result in the premature deletion of unexpired records. Therefore, Cohasset recommends the use of automated Project-level Liens within the regulated entity's environment to enforce governance policies; otherwise, procedural controls and monitoring are required to scrutinize privileged administrative actions which may result in the premature deletion of records.

2.2.3.7 Security

- Independent third-party audits of Google's infrastructure, services and operations are undertaken on a regular basis to verify security, privacy and compliance controls which were built with a Zero Trust approach.
- Google Authentication Services provides authentication for users within the AODocs environment.
- AODocs Compliance Archive utilizes the HTTPS protocol to communicate between services, and communications are encrypted in transit with Transport Layer Security (TLS) The communication between GCS Buckets (i.e., when copying snapshots between the Temporary GCS Bucket and long-term GCS Buckets) utilizes the Application Layer Transport Security (ALTS) protocol.
- By default, GCP encrypts all data at rest within the AODocs Multi-Tenant Datastore and BigQuery databases, utilizing the AES-256 data encryption algorithm. Data is encrypted prior to being written to disk, then divided into chunks and encrypted again at the storage level with an individual encryption key for each chunk.
- Records and their properties are encrypted at rest on GCS. The GCS Buckets reside in an environment controlled by the regulated entity and as such, the regulated entity can elect to use their own encryption keys.

2.2.3.8 Clock Management

- AODocs and GCS use TrueTime, Google's globally synchronized clock, which keeps strong consistency across the clocks in its data centers and tracks a time interval with bounded time uncertainty that is guaranteed to

contain the clock's actual time. TrueTime's bounded time uncertainty is expressed in milliseconds and is documented as varying about 1 to 7 milliseconds in the Google production environment, assuring that timestamps are accurate when the data and metadata are fully written.

- Google assures that neither end users nor system administrators have the ability to manipulate system time on the Google Cloud Platform. These controls prevent any inadvertent or intentional administrative modifications of clocks, which could allow for premature deletion of protected records.

2.2.4 Additional Considerations

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

- Properly configuring Google Workspace (which includes Google Drive), AODocs, and Google Cloud Storage (GCS) environments as outlined above to ensure a compliant storage environment.
- Creating Compliance Archive Retention Schedules that meet regulatory requirements, and assigning them to AODocs libraries, folders or sub-folders, to ensure retention controls are applied to records.
- Finalizing records to ensure they are copied from the collaborative Drive and AODocs environments to immutable storage in a locked GCS Bucket.
- Applying the *On Hold* flag for finalized records or otherwise preserving records for legal matters, government investigations, external audits and other similar circumstances, and removing the *On Hold* flag when the applicable action is completed.
- Ensuring that appropriate administrative procedures are in place to regularly monitor error notifications and immediately remedy both human-originated and system-originated exceptions which may occur during the lifecycle of required records.
- Establishing procedural controls and monitoring of administrative actions such as (a) directly accessing the GCS Buckets storing AODocs-controlled records, (b) removing non-automated Project-level Liens, and (c) deleting GCS accounts, Projects, and Buckets and/or Google Workspace domains or user accounts, including the AODocs service account.
- Establishing procedural controls to restrict storage administrator actions which may result in the removal of (a) a custom Google Drive Label of *Archive in Progress* and (b) view-only permissions from Google Drive Attached Files, prior to their preservation in a locked GCS Bucket.
- Maintaining their **GCP *Account layer*** (Organization, Folder and Project) and paying for appropriate services, until their retention periods have expired or until the records have been transferred to another compliant storage system. Similar to decommissioning a datacenter, deleting a Project in the Account layer will delete Buckets and records, even if the record is *not* eligible for deletion. As a safeguard:
  - Setting an automated Project-level *Lien*, which is inherited by its Buckets, to prohibit Bucket deletion while the *Lien* is in place.
  - When using non-automated Project-level Liens, restricting the assignment of the ***resourcemanager.projects.updateLiens*** permission to one or more individuals, who are separate from administrators responsible for day-to-day management of the Google environment to prevent the removal of *Liens*.

- Maintaining their **AODocs account** in good standing to ensure that protection of records continues until their retention periods have expired and associated legal holds have been released. Should the regulated entity discontinue its use of AODocs prior to the expiration of the retention period and any associated legal holds, the regulated entity must assure that the records, associated properties (metadata), and audit logs are transferred to another compliant storage media prior to the deletion of records from AODocs and GCS.

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[18] with AODocs Compliance Archive 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 Workspace Capabilities

The recording and post-recording verification processes of Workspace with AODocs Compliance Archive are described below.

2.3.3.1 Recording Process

- AODocs Compliance Archive is built natively upon the Google Cloud Platform and retains required records in Google Cloud Storage (GCS). As such, Google's advanced electronic recording technology applies a combination of checks and balances to assure that records are written in a high quality and accurate manner.
  - During the Google DWT export of Attached Files, including system metadata, for storage in GCS, checksums are calculated at multiple levels (i.e., at individual file-level, as well as for the entire zip file) to assure that the files are written in an accurate manner. Note: *Native Google Drive files are first converted to Microsoft Office format during the export process and a file-level checksum is then calculated for each file*.
  - Additionally, when a snapshot of the finalized AODocument is written as a payload.json file to the GCS Bucket, checksums are calculated to assure a high-quality and accurate write.

[18] Google functionality includes (a) Google Workspace to authenticate users and provide collaboration, (b) Google Drive to store working copies of native content (i.e., Google Docs, Sheets and Slides) and non-native content (i.e., other Google Drive files, such as PDFs, images and video), (c) Google Cloud Storage for final records, and (d) other Google services.

- If an error occurs during either the creation of the Google DWT zip file or the write to the Temporary GCS Bucket, errors are logged in an error report in the Temporary GCS Bucket and must be manually corrected.
  - In the event Attached Files exceed allowable size limitations, the write operation is rejected and an error is logged in an error report in the Temporary GCS Bucket. Manual action must be taken, via a dedicated user interface, to upload the files to GCS.
- If an error is identified during the AODocs-initiated write process in GCS (i.e., during the decompression of the zip file and copy to long-term GCS Buckets) attempts are made to auto-correct, a notice is sent to AODocs super administrators, and the exception is entered in the audit log. If autocorrection is unsuccessful, manual action must be taken to correct the situation.
- Checksums are stored as critical system metadata to enable post-recording integrity verification and automated object repair.

2.3.3.2 Post-Recording Verification Process

- Within GCS, checksums are validated (fixity checks) on access and regular data integrity checks/fixity 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).
  - GCS is designed to assure 11-nines (99.999999999%) of durability for all storage classes.
- When a record is retrieved, if any part of the data is incorrect, the GCS durability features will recover or regenerate an accurate replica.

2.3.4 Additional Considerations

The source system is responsible for transmitting the complete contents of the required records and Google validates the accuracy of the recording process.

2.4 Capacity to Download and Transfer Records and Location Information

2.4.1 Compliance Requirement

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.

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]

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[19] with AODocs Compliance Archive meets this SEC requirement to maintain 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 Workspace Capabilities

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

- Each record stored in GCS is assigned a GCS Global Identifier, which facilitates findability. Specifically, the following metadata is captured for each record and immutably retained for the duration of the applied retention period.
  - The Bucket name, which is unique across the entire GCS namespace,
  - A record name, which is unique within the Bucket, and
  - A GCS storage timestamp
- Google Cloud Platform assures that hardware and software capacity allow for ready access to the records and properties (indexes and metadata). Further, Google 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 utilized by the regulated entity.
- When a record is written to a GCS Bucket, a Retention Document is automatically created within the AODocs Retention Library to serve as an index for the record. The Retention Document stores links between the AODocument, the source Google Drive files (i.e., Attached Files), and the records stored in GCS. Each Retention Document includes (a) an AODocs unique ID, (b) an AODocs Event Date (i.e., the date an object was finalized as a record), and (c) the GCS Global Identifier. Additional key index properties include:

Properties	Description
Record category	A meaningful label depending on the business case, for example, "Taxes"
Folder	A logical subset of an AODocs Library, used to organize and manage AODocuments and any Attached Files.
Lifecycle State	The lifecycle state is set to control for finalized AODoc Documents and their Google Drive attachments
Retention Time	Number of years before the documents are eligible for disposition

[19] Google functionality includes (a) Google Workspace to authenticate users and provide collaboration, (b) Google Drive to store working copies of native content (i.e., Google Docs, Sheets and Slides) and non-native content (i.e., other Google Drive files, such as PDFs, images and video), (c) Google Cloud Storage for final records, and (d) other Google services.

Properties	Description
[AODocs] Event	A property used to determine how the start of the retention period is determined. For required records, the "triggering event" occurs when an AODocument and Attached Files are finalized and snapshots are immutably stored in a GCS Bucket
Target Destruction Date	Date at which the AODocument will be eligible for deletion
On hold	Switch to suspend the Retention Schedule for a document
Retention ID	The unique identifier assigned to a retention schedule, comprised of a policy code and country code (e.g., ADM156-US)
Source library ID	The ID of the library where the snapshot has been taken
Source class ID	The ID of the class where the snapshot has been taken
Source document ID	The ID of the document for which a snapshot has been taken
GCS objects	An array of links to the objects stored on Google Cloud Storage
GCS objects checksum	Checksums of the objects once they are stored on Google Cloud Storage nearline bucket
Google Drive objects checksum	Checksums of the content prior to being written to Google Cloud Storage
Source document creator	The creator of the original document
Source document trigger author	The user who triggered the document finalization
Process Start Date	The start date of the document finalization process
Process Conclusion Date	The end date of the document finalization process

Note: In addition to the properties listed above, the finalized AODocument contains links to system properties for each Google Drive Attached File, including title of document, creator and AODocs Event Date (snapshot creation date/time).

- Retention Documents are natively protected as read-only for all users, except super administrators. Should a super administrator remove a Retention Document from the Retention Library, the action will be logged to allow for recovery. See Section 2.8, *Organization and Accuracy of Indexes*, for additional details.
  - AODocs automatically retains two copies of the Retention Library, when a second, optional Retention Library has been configured for the regulated entity's Google Workspace Domain (see Section 2.2.3.3, *Retention-related Configurations,* for more information).
  - By default, properties (indexes and metadata) stored in the Retention Document, are retained until the record's assigned Target Destruction Date has passed.
- Records are retained in GCS Buckets with the *Bucket Lock* feature enabled. To search for and download records from a GCS Bucket, an AODocs administrator or super administrator must perform the following steps:
  - Search the AODocs Retention Library (a) using search capabilities provided on the AODocs user interface or (b) via APIs, to locate the desired records.
  - The administrator then selects one or more items from the resulting list of records and downloads them from GCS as follows:
    - Snapshots of native Google Workspace files (e.g., Docs, Sheets, Slides) are downloaded in Microsoft Office format, without associated metadata or properties.

- Snapshots of non-native objects are downloaded in their original format (e.g., DOC, XLS, PDF, MP4), without associated metadata or properties.

2.4.4 Additional Considerations

The regulated entity is responsible for (a) maintaining its Google and AODocs accounts in good standing, (b) authorizing user privileges, (c) maintaining appropriate technology and resource capacity, encryption keys, and other information and services needed to use Workspace with AODocs Compliance Archive 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.

Additionally, the regulated entity must establish procedures to regularly monitor error notifications and immediately remedy exceptions which may limit the ability to locate required records.

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.[20] [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.[21] [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.

[20] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66421.

[21] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66421.

2.5.2 Compliance Assessment

Cohasset upholds that the functionality of Google[22] with AODocs Compliance Archive meets both paragraphs (A) and (B) of this SEC requirement by retaining a persistent duplicate copy of the records or alternate source to reestablish the records, when the considerations described in Section 2.5.4 are satisfied.

2.5.3 Workspace 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, GCS Buckets, with the *Bucket Lock* feature enabled, are used to immutably retain records for the required retention period.
- When an AODocs Retention Schedule is first created, (a) a primary GCS Bucket is automatically created in a GCS Nearline Storage Class and assigned the Retention Time associated with that AODocs Retention Schedule and (b) a secondary GCS Bucket, configured as an exact duplicate of the primary Bucket, including all applied controls, is automatically created in a GCS Coldline Storage Class.
- Records are written to both the primary and secondary GCS Buckets and are immutably retained according to the assigned Retention Time. Should a non-recoverable error occur in the primary Bucket, a record may be recovered from the secondary Bucket.

2.5.3.2 Other Redundancy Capabilities

- For compliance with paragraph (B), GCS uses erasure coding, which stores coded segments of the record across multiple disks located in different disks, racks, and availability zones (i.e., separate power and network failure domains). In the event of an error, an accurate replica of the full record can be regenerated.
- Erasure coded data segments are retained, at a minimum, for the time period applied to the GCS Bucket.

2.5.4 Additional Considerations

Additionally, the regulated entity is responsible for (a) maintaining its Google and AODocs accounts in good standing and (b) maintaining the technology, storage capacity, encryption keys, and other information and services needed to permit storage of and access to the redundant records.

[22] Google functionality includes (a) Google Workspace to authenticate users and provide collaboration, (b) Google Drive to store working copies of native content (i.e., Google Docs, Sheets and Slides) and non-native content (i.e., other Google Drive files, such as PDFs, images and video), (c) Google Cloud Storage for final records, and (d) other Google services.

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[23] with AODocs Compliance Archive 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 Workspace Capabilities

The regulated entity is responsible for providing adequate facilities and technology to produce records for examination and compliance is supported by Google with AODocs Compliance Archive.

- GCS encrypts data at rest and automatically decrypts the data, as part of the process of rendering the data for use. By default, GCS maintains the encryption key for data at rest.
- Regulated entity administrators may search for records retained within GCS Buckets, as described in Section 2.4.3, and download selected records.
- Once downloaded, a viewer or other local capabilities (i.e., Microsoft Office applications for native files converted to the Microsoft Office format) may be used to render a human-readable projection or print of the records.

2.6.4 Additional Considerations

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

[23] Google functionality includes (a) Google Workspace to authenticate users and provide collaboration, (b) Google Drive to store working copies of native content (i.e., Google Docs, Sheets and Slides) and non-native content (i.e., other Google Drive files, such as PDFs, images and video), (c) Google Cloud Storage for final records, and (d) other Google services.

2.7 Provide Records to Regulators

2.7.1 Compliance Requirement

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

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[24] with AODocs Compliance Archive supports the regulated entity in meeting this SEC requirement to immediately provide regulators with reproductions of the records.

2.7.3 Workspace Capabilities

The regulated entity is responsible for producing records for regulators, and compliance is supported by Google with AODocs Compliance Archive.

- Authorized users may conduct searches using the AODocs Retention Library, and download records from GCS, as described in Section 2.4.3, *Capacity to Download and Transfer Records and Location Information*
- Records can then be viewed or printed as follows:
  - Native files can be viewed in Microsoft Office applications, a browser, or imported into Google Workspace and, thereafter, native Google tools may be used to reproduce the object.
  - Non-native files may be viewed in Microsoft Office applications, or via a browser or other local capabilities.
- Human-readable productions of native and non-native files may be provided to regulators by the regulated entity.

2.7.4 Additional Considerations

The regulated entity is responsible for providing the records to the regulator in the requested format.

[24] Google functionality includes (a) Google Workspace to authenticate users and provide collaboration, (b) Google Drive to store working copies of native content (i.e., Google Docs, Sheets and Slides) and non-native content (i.e., other Google Drive files, such as PDFs, images and video), (c) Google Cloud Storage for final records, and (d) other Google services.

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[25] with AODocs Compliance Archive, supports the regulated entity's efforts to meet this SEC requirement for an audit system.

2.8.3 Workspace Capabilities

The regulated entity is responsible for an audit system, and the following functionality supports the regulated entity in meeting this requirement.

- The following audit information is immutably retained for each record stored in GCS, for the same duration as the record:
  - A GCS Global Identifier that is comprised of (a) the Bucket name, which is unique across the entire GCS namespace and (b) a record name, which is unique within the Bucket.
  - The GCS creation (storage) timestamp.
- The record content stored in GCS is immutable, meaning modifications are disallowed; therefore, tracking of the inputting of changes made is not relevant.
- In addition to the immutable data in GCS, AODocs creates and preserves extensive Retention Audit Logs related to: (a) the capture, storage, and management of records and (b) administrative and system events. Retention Audit Log entries relate to the retention of records and include, but are not limited to:
  - Creating a Retention Schedule.
  - Applying or removing a Retention Schedule to/from a library or folder.

[25] Google functionality includes (a) Google Workspace to authenticate users and provide collaboration, (b) Google Drive to store working copies of native content (i.e., Google Docs, Sheets and Slides) and non-native content (i.e., other Google Drive files, such as PDFs, images and video), (c) Google Cloud Storage for final records, and (d) other Google services.

- Storing a record with its assigned retention duration and Target Destruction Date in a GCS Bucket, via the DWT export process, and applying retention controls.
- Applying or removing a legal hold.
- Deleting eligible, finalized AODocuments along with any attached source Google Drive files.
- Deleting eligible Retention Documents from AODocs.
- Administrative and system event log entries include, but are not limited to:
  - System errors, such as the unavailability of a system or subsystem, checksum errors, insufficient storage space, and failure of key processes such as DWT export.
  - Human-originated exceptions, such as administrative deletion of Retention Classes, Libraries, Log Class and/or a Log document.

  For each audit entry, key information is captured such as Unique ID (UUID) for the entry, a log message identifying the performed operation, user performing operation, Library, Class, Document ID, timestamp and hash to prove consistency of message.

- Retention Audit Log entries are permanently retained within both the AODocs BigQuery storage, in a secured, dedicated dataset, and in the Retention Audit Log Library. Additionally, the Retention Audit Log Library is backed up weekly to a GCS Bucket in cold storage to assure availability.
- Authorized system administrators for the regulated entity can search Retention Audit Log events and filter by user, date range, type of event, etc., then:
  - View the results of the search on the Retention Audit Log user interface.
  - Export select Retention Audit Log events via the AODocs API.

2.8.4 Additional Considerations

The regulated entity is responsible for maintaining an audit system for inputting records and changes made to the records and for keeping the audit events for the same time period as the associated record. In addition to relying on the immutable metadata, the regulated entity may utilize the Retention Audit Log.

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

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*

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

and locate records preserved by means of the electronic recordkeeping system."[26]

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[27] with AODocs Compliance Archive 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 Workspace Capabilities

The regulated entity is responsible for this requirement for information needed to locate the records, and the following functionality supports the regulated entity in meeting this requirement.

- When a record is written to a GCS Bucket, AODocs stores the following properties (indexes and metadata) for the record in the form of a Retention Document, within the AODocs Retention Library. Key properties include:

Properties	Description
Record category	A meaningful label depending on the business case, for example, "Taxes"
Folder	A logical subset of an AODocs Library, used to organize and manage AODocuments and any attached Google Drive files
Lifecycle State	The lifecycle state is set to control for finalized AODoc Documents and their Google Drive attachments
Retention Time	Number of years before the documents are eligible for disposition
[AODocs] Event	A property used to determine how the start of the retention period is determined. For required records, the "triggering event" occurs when an AODocument and its attachments are finalized and a snapshot is immutably stored in a GCS Bucket
[AODocs] Event Date	The date when immutable retention begins
Target Destruction Date	Date at which the document will be eligible for deletion
On hold	Switch to suspend the Retention Schedule for a document
Retention ID	The unique identifier assigned to a retention schedule, comprised of a policy code and country code (e.g., ADM156-US)
Source library ID	The ID of the library where the snapshot has been taken
Source class ID	The ID of the class where the snapshot has been taken
Source document ID	The ID of the document for which a snapshot has been taken
Snapshot version	The version of the snapshot
GCS objects	An array of links to the objects stored on Google Cloud Storage
GCS objects checksum	Checksums of the objects once they are stored on Google Cloud Storage nearline bucket
Google Drive objects checksum	Checksums of the content prior to being written to Google Cloud Storage

[26] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66424.

[27] Google functionality includes (a) Google Workspace to authenticate users and provide collaboration, (b) Google Drive to store working copies of native content (i.e., Google Docs, Sheets and Slides) and non-native content (i.e., other Google Drive files, such as PDFs, images and video), (c) Google Cloud Storage for final records, and (d) other Google services.

Properties	Description
Source document creator	The creator of the original document
Source document trigger author	The user who triggered the document finalization
Process Start Date	The start date of the document finalization process
Process Conclusion Date	The end date of the document finalization process

Note: In addition to the properties listed above, the finalized AODocument (Source Document) contains links to system properties for each Google Drive file attachment, including title of document, creator and AODocs Event Date (snapshot creation date/time).

- AODocs retains the Retention Document in a read-only state for the same retention period as the record. Note: Super administrators have special privileges which allow them to remove contents from the Retention Library; should this occur, the action is logged to allow for recovery of the data.
- Contents of the Retention Library can be searched via AODocs search tools or APIs. A list of Retention Documents matching the search criteria may be viewed and/or exported as a CSV file. See Section 2.4 *Capacity to Download and Transfer Records and Location Information* for additional information.
- When a second, optional Retention Library has been configured for the regulated entity's Google Workspace Domain, AODocs maintains two copies of the Retention Library, ensuring that in the event properties (indexes and metadata) stored in the primary Retention Library are lost or damaged, the contents of the Retention Library can be recovered from the duplicate. Additionally, Cohasset believes that AODocs further meets this SEC requirement through the use of erasure coding (i.e., provided automatically by the Google Cloud Platform). Data written to the Retention Library is written in coded segments across different disks, racks, and availability zones (i.e., separate power and network failure domains). In the event of a hardware error, an accurate replica of the properties (indexes and metadata) can be regenerated.

2.9.4 Additional Considerations

The regulated entity is responsible for (a) maintaining its Google and AODocs accounts in good standing, (b) authorizing user privileges, (c) maintaining appropriate technology and resource capacity, encryption keys, and other information and services needed to use Workspace with AODocs Compliance Archive to readily access, download, and transfer the information needed to locate the records, and (d) 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

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.

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"):
*****

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 Workspace Capabilities

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

2.10.4 Additional Considerations

There are no additional considerations related to this requirement.

3 • Assessment of Google Compliance Archiving Support for Digital Communications and Oral Conversations

This section presents Cohasset's assessment of the functionality of Google's Digital Communications Governance and Archiving (DCGA) Export Service and Domain Wide Takeout (DWT) Export Service to support the regulated entity in meeting its compliance requirements for digital communications and oral conversations, when a required record.

Regulated entities must meet stringent regulatory mandates for digital communications and certain recordings of oral conversations, when a required record. Mandates include, but are not limited to, monitoring and supervisory review processes aimed at ensuring adherence to regulatory standards and ethical practices.

Given the rigorous requirements, the vast volume of different sources and types of electronic communications, and the need for efficiency, most firms rely on technological solutions to facilitate these supervisory reviews. Rather than providing native monitoring and supervision services, Google has opted to deliver advanced automated capabilities through the Google DCGA and DWT Export Services, which enable the efficient export of digital communications and oral conversations to third-party Digital Communications Governance and Archiving (DCGA) platforms.

Accordingly, this section of Cohasset's report assesses Google's export services in supporting the regulated entity with compliance for digital communications and oral conversations, by automating the process of exporting these artifacts to third-party platforms to preserve, monitor, supervise, and manage.

3.1 Overview of the Regulatory Requirements for Digital Communications and Oral Conversations

Multiple regulatory bodies oversee certain financial services communications, including, but not limited to, (a) SEC for registered investment advisors, broker-dealers, securities-based swap dealers and major security-based swap participants, (b) FINRA for broker-dealers, and (c) CFTC for commodity future trading and entities regulated by Commodity Exchange Act or CFTC regulations. Additionally, recordings of certain oral conversations may be required records, such as recordings for compliance with FINRA Rule 3170, Tape Recording of Registered Persons by Certain Firms, and recordings kept for one year for compliance with CFTC regulation 17 CFR 1.31. These mandates include but are not limited to (a) retaining required communication artifacts for the stipulated retention period, (b) implementing monitoring and supervisory review processes, and (c) retaining required digital communication artifacts in a format and media that complies with the electronic recordkeeping system requirements.

The following table highlights selected regulations. As noted in the grey heading rows, refer to the noted subsection of Appendix B, *Overview of Relevant Requirements for Digital Communications and Oral Conversations*, for excerpts of these regulations.

Rule	Brief Summary
SEC Rules for Broker-Dealers, Securities-Based Swap Dealers and Major Security-Based Swap Participants	Summarized below; for excerpts of these regulations refer to Appendix B.1, *Overview of SEC Digital Communications Requirements for Broker-Dealers, Securities-Based Swap Dealers and Major Security-Based Swap Participants*
SEC Rule 17a-4, paragraph (b) SEC Rule 18a-6, paragraph (b)	• Requires preservation of communications received and communications sent, including, but not limited to inter-office memoranda and communications relating to its business as such. • Includes sales scripts and recordings of telephone calls required to be maintained pursuant to section 15F(g)(1) of the Act (15 U.S.C. 78o-10(g)(1)). • Requires digital communications to comply with the electronic recordkeeping system requirements specified in Rule 17a-4(f) and 18a-6(e), respectively.
15 U.S.C. 78o-10, paragraph (g)	• Stipulates that required recorded communications for security-based swap dealers and major security-based swap participants include electronic mail, instant messages, and recordings of telephone calls.
SEC Rule 17a-4, paragraph (f) SEC Rule 18a-6, paragraph (e)	• Defines requirements for electronic recordkeeping systems retaining required books and records. • For additional information, see Section 2, *Assessment of Google Workspace with AODocs Compliance Archive for Compliance with SEC Rules 17a 4(f) and 18a 6(e).*
FINRA Rules	Summarized below; for excerpts of these regulations refer to Appendix B.2, *Overview of FINRA Requirements for Digital Communications and Oral Conversations*
FINRA Rule 3110, *Supervision,* paragraph (b)	• Requires supervision of business activities, including monitoring and supervisory review of incoming and outgoing written (including electronic) correspondence and internal communications relating to the member's investment banking or securities business and the activities of associated persons.
FINRA Rule 2210, *Communications with the Public*	• Categorizes communications into retail communications, correspondence, and institutional communications. • Sets standards for monitoring and supervisory review. • Requires compliance with the retention period stipulated by Rule 17a-4(b) and the format and media stipulated by Rule 17a-4(f).
FINRA Rule 3170, *Tape Recording of Registered Persons by Certain Firms* FINRA Rule 3170 Guidance	• Enhances oversight and surveillance of firms hiring registered representatives with a history of compliance issues. • Mandates that certain firms record and retain telephone conversations between their registered persons and customers. • Requires supervisory review of the recordings of telephone conversations and reporting of findings to FINRA.
SEC Registered Investment Advisor Rules	Summarized below; for excerpts of these regulations refer to Appendix B.3, *Overview of SEC Digital Communications Requirements for Investment Advisors*
SEC Rule 204-2, paragraph (a)	• Requires preservation of certain types of written communications, including communications related to recommendations, transactions, and performance.
SEC Rule 206(4)-7	• Requires compliance procedures and practices, which includes monitoring and supervision of communications.
SEC Rule 204-2, paragraph (g)	• Defines requirements for electronic storage retaining required books and records. Note: These requirements are less-restrictive than the requirements of SEC Rules 17a-4(f) and 18a-6(e), which is addressed in Section 2, *Assessment of Google Workspace with AODocs Compliance Archive for Compliance with SEC Rules 17a 4(f) and 18a 6(e).*

Rule	Brief Summary
CFTC Rules	Summarized below; for excerpts of these regulations refer to Appendix B.4, Overview of CFTC Communications Requirements
CFTC Rule 1.31	• Addresses the retention and production of records • Sets a general fixed retention period of 5-years and an explicit retention period of 1-year for certain required oral conversations.
CFTC Rule 1.35, paragraph (a)	• Requires retention of records of commodity interest and related cash or forward transactions, including oral and written communications provided or received by telephone, voicemail, facsimile, instant messaging, chat rooms, electronic mail, mobile device, or other digital or electronic media.

3.2 Google DCGA Export Services for Digital Communications

The DCGA Export Service is designed to automate the process of journaling the following types of digital communications for monitored users to the DCGA platform selected by the regulated entity.

- Gmail messages, including outbound and inbound email messages and Google Calendar invitations sent to meeting participants.
- Google Chat messages, including both (a) direct messages (i.e., DMs) for one-to-one and one-to-many small group communications and (b) persistent chat spaces for posting team-based communications. Note: In-Meeting Chats are excluded from this assessment.
- Google Calendar events, e.g., event name, date, time, location, description, links to attachments, and reminders associated with those events.

It is Cohasset's opinion that the functionality of Google with the DCGA Export Service supports the regulated entity in meeting its digital communications requirements, when configured and implemented, as described in this section.

3.2.1 Configuration of DCGA Export Service for Digital Communications

The regulated entity is responsible for identifying the users whose communications are required books and records, then designating the monitored users by OU or Group, as described in the following table, which lists the Workspace service-specific licensing and configurations required to enable the Google DCGA Export Service.

	Workspace Configurations for the Google DCGA Export Service		
	Gmail Messages	Google Chat Messages	Calendar Items
Licensing	• Requires enterprise license for business users. • No add-on licenses are required.		• Requires an enterprise license for business users **plus** an *Assured Controls* add-on license per user.

<table>
<tr><th></th><th colspan="3">Workspace Configurations for the Google DCGA Export Service</th></tr>
<tr><td>Setting up Monitoring Policies</td><td colspan="3">The regulated entity's Workspace administrator sets up monitoring policies, as follows, to enable DCGA monitoring.</td></tr>
<tr><td></td><td>● Selecting the Third-party email archiving option from the Gmail Routing menu.
● Designating the Organizational Unit (OU) or Group to be monitored.
● Providing one or more target email addresses for the third-party DCGA platform(s).
<u>Notes</u>: Care must be taken to ensure the email address(es) are accurate and appropriate. Additionally, if the maximum limit of 5,000 to 10,000 export messages per day will be exceeded, the regulated entity must introduce different destination email addresses for different OUs or Groups; each with a manageable number of users.</td><td>● Selecting the Third-party email archiving option from the Chat Third-party Archiving settings menu.
● Designating the OU or Group to be monitored.
● Providing one target email address for the third-party DCGA platform.
<u>Note</u>: Care must be taken to ensure the email address is accurate and appropriate.
● Selecting the archival frequency, i.e., every 1-24 hours.</td><td>● Setting the Third-party archiving enabled attribute to True on the Third-party Archiving settings menu.
● Specifying the OU or Group to be monitored.
● Providing one target email address for the third-party DCGA platform.
<u>Note</u>: Care must be taken to ensure the email address is accurate and appropriate. Multi-person authorization is required when entering or updating the email address to prevent potential security risks.</td></tr>
<tr><td>Chat History</td><td>● N/A</td><td>● Chat history must be enabled for the OU or Group, which allows the Google DCGA Export Service to export chat messages.
● Additionally, the option for users to change their own history setting must be disallowed.</td><td>● N/A</td></tr>
<tr><td>Disabling Monitoring Policies</td><td colspan="3">● DCGA Monitoring may be turned off at any time by the administrator, and administrators may remove users from the monitored OU or Group. Therefore, procedural controls and monitoring of administrative actions are required to scrutinize changes which may result in disabling or removing DCGA monitoring for some or all OUs or Groups.</td></tr>
<tr><td>Setting up custom headers</td><td>● Optionally, customized email headers may be configured to insert metadata in message headers to improve message tracking and organization.
● Custom header metadata may be programmatically inserted by:
○ Application code,
○ An on-prem MTA (Mail Transfer Agent), or
○ A Gmail compliance rule.</td><td>● Optionally, entering a comma-separated list of custom headers required by the DCGA platform to uniquely identify Chat messages.</td><td>● N/A</td></tr>
</table>

	Workspace Configurations for the Google DCGA Export Service		
Security	• Recommend configuring Transport Layer Security (TLS) compliance to encrypt data in transit.	• Enable TLS compliance settings to require secure TLS connections to encrypt data in transit.	• Enable TLS compliance settings to require secure TLS connections to encrypt data in transit.

3.2.2 Record Definition and DCGA Export Process for Digital Communications

For each type of digital communication, the following subsections detail: (1) the journaling process, (2) elements archived in the journaled message or event, and (3) archive planning considerations.

3.2.2.1 Gmail Messages

Using the configurations described in Section 3.2.1, *Configuration of DCGA Export Service for Digital Communications*, when Gmail messages are journaled for a monitored user, the Google **DCGA Export Service** *blind-copies* the Gmail message contents and associated metadata in one file, for ingestion by a third-party DCGA platform. Journalling of inbound, outbound and internal Gmail communications is performed by the Google DCGA Export Service according to the following process:

- For each email user in a monitored OU or Group, a journal copy of the Gmail message content and associated metadata is created when a message is sent (i.e., outbound emails) and a journal message is created for each monitored recipient when the Gmail message is received (i.e., inbound emails). Note: Internal Gmail messages are handled as inbound for recipients and outbound for the sender.
  - Journaled messages are created only for those Gmail users in a monitored OU or Group, as well as monitored users added as a recipient, via a routing rule.
  - If the owner of a delegated mailbox is monitored, all messages sent and received via the delegated mailbox are journaled. If the owner of a delegated mailbox is not monitored, messages received are not journaled, however, messages sent on behalf of the mailbox owner, by a delegate who is monitored, are journaled.
  - Messages sent or received by monitored users using collaborative mailboxes are journaled.
  - Messages saved as ***drafts*** are not journaled.
  - When Confidential Mode is set on an email message, attachments are supported, however, recipients cannot download, print, or forward the attachments. Confidential Mode controls do not prevent the message from being (a) added to the Google message queue or (b) exported by the Google DCGA Export Service. Accordingly, even if the source message has expired and is no longer available, the message will be exported by the Google DCGA Export Service.
- Journaled messages are stored in a Google message queue until the next scheduled SMTP export by the Google DCGA Export Service. See Section 3.5, *Record Redundancy*, for additional details.

The following table defines a Gmail message by detailing the Gmail message contents and associated metadata that are journaled as a fully formed RFC 5322/MIME message. This journal file for each inbound, outbound and internal Gmail communication is transmitted to a third-party DCGA platform for ingestion.

	Elements Archived in the Journaled Gmail Message
Message header (message metadata)	● The Gmail message header retains important metadata about the message, including: ○ Message-ID (message identifier, which is unique across the Google email platform) ○ Message timestamp ○ From, which lists the original message author(s) ○ Sender, if the message is sent "on behalf of" another user ○ To, CC and BCC, lists recipients and whether the message was sent directly to them or if they were cc'd or bcc'd. (See row entitled *Distribution lists* for information on distribution list expansion) ○ Subject of the email message ▪ When the subject includes emojis, the emoji itself is part of the message reaction content (Unicode).
Customized message header (message metadata)	● Customized header metadata is used by downstream processes to enhance search and select messages for specific purposes. For example, inserting X-Case-ID custom metadata, in both outbound and inbound messages, allows the archive to associate these messages by case, even if the subject is changed or users remove the *Re:* prefix. ● When customized header metadata is configured, it is journalled with the Gmail message.
Distribution lists	● For distribution lists (a.k.a., Groups or address-lists): ○ The message journaled for the sender includes only the distribution list name. ○ The message journaled for the recipient shows the recipient's email address and the distribution list name used when sending the message. For example: `To: user1@domain.com, Expanded: distribution_list@domain.com` ○ Google follows the standard Internet-message (RFC 5322), which disallows nested Groups and sets header line-length limits. Additionally, Google attempts to expand distribution lists via annotations to the message body.
Message content and attachments	● The message content contains the body of the email message, including: ○ Content typed or inserted into the message body. ○ Links to webpages and other external content. ● Message attachments are either (a) a link (i.e., a pointer) or (b) an immutable uploaded file and included in the message body. ○ When a link points to a native Workspace Doc, Sheet or Slide that is stored in Drive; the link contains a reference to the attachment ID, which is used to retrieve the attachment separately. ○ An uploaded file (e.g., images, PDFs, Word documents and CSV files) are physically uploaded and attached/embedded in the message body. Attachments are not compressed or reformatted in any way.
Message Reactions	● When using the Gmail client, both senders and recipients of the message can append a reaction and later change or remove the reaction. ○ Reactions to a message, or modifications to a reaction, are considered distinct messages and are journaled separately. Note: If a reaction is added and/or modified within the specified "undo send" period (i.e. between 5 and 30 seconds), the reaction or modification to a reaction is not journaled. ○ If a reaction is subsequently removed, the separate journaled message used to add the reaction is not removed, nor is a new journaled message created. Rather, the removed reaction is treated as a UX (User Experience) and interpreted by the Gmail client during rendering.
@Mentions	● @username text typed in an email subject or body is preserved, as it is written; there is no separate @Mention field. ● If the Gmail rich text editor is used to insert an @Mention, the journaled message content will include the HTML anchor tag (e.g. @John Doe).

	Elements Archived in the Journaled Gmail Message
Emojis	● Emojis may be embedded in the subject or body of a Gmail message. ● Gmail stores the Unicode code for each emoji, and the renders it as the corresponding graphic. ● Reactions to emojis are treated as separate messages in the message thread and are journaled separately; see *Message Reactions* row, above.
Photos	● When photos are attached to a journaled email, the entire raw message with all of its MIME parts is sent to the journal archive (i.e., the full binary data of the photo attachment is included).
Signatures	● Text-based signatures are considered part of the message body and included with the journaled message. ● Signatures with embedded images are treated as an attachment to the message and journaled as such.
Labels	● Labels are not journaled; they are considered an inbox organization feature and therefore, not considered part of the message.

When planning the process of journaling Gmail messages using the DCGA Export Service, the regulated entity is responsible for:

1. Evaluating how organizational policies may affect outbound and inbound Gmail messages and journaling, keeping in mind organizational policies may differ by OU or Group, potentially causing different behaviors for the sender and each recipient.

Type of Organizational Policy and Use	Impact on journaling
Pre-delivery malware/antivirus policies scan attachments and automatically take a specified action (e.g., quarantine or modify/deliver the message) when the policy is violated.	● Inbound messages that are accepted by the Gmail service are journaled when delivered to the inbox. ○ If a content compliance rule modifies a received message, the message is journaled only after all content compliance rules have been applied. ○ Inbound messages that are quarantined are not journalled until an administrator releases the message from quarantine. ○ Inbound messages that are ultimately rejected (i.e., denied outright and never released from quarantine) are not journaled. Reminder: The recipient never receives these messages in their mailbox. ● Outbound messages are journaled when sent, before any action is taken to quarantine, reject or modify the message. ○ Outbound messages that are modified as part of a content compliance policy include the original content as sent by the user (i.e., if an attachment is removed by a compliance policy, the journaled copy still retains the attachment). Note: Internal messages are handled as inbound for recipients and outbound for the sender.
Attachment compliance policies scan attachments (by file type, file name, or total message size) and automatically take a specified action (e.g., reject, quarantine, or modify/deliver the message) when the policy is violated.	
Content compliance policies examine the headers, message body, and attachments and automatically take a specified action (e.g., reject, quarantine, modify, or deliver the message) when certain conditions are met.	
Objectionable Content policies scan messages for objectionable words or phrases and automatically take a specified action (e.g., reject, quarantine, or modify/deliver the message) when certain conditions are met.	
Routing rules define (a) default delivery path for messages and (b) targeted delivery rules to modify or redirect messages based on specific criteria,	● Because routing rules are used to journal messages, the priority order and scope of routing rules directly impact the journalled messages.

2. Monitoring administrator alerts for journaled messages that fail delivery to the DCGA email address; any Gmail messages not flagged as a failed delivery were successfully transmitted to the DCGA platform.
    - When delivery fails for a journaled message, the SMTP host returns a temporary error, and the Gmail service attempts to resend the message for 8 days. If delivery remains unsuccessful, the SMTP host returns a permanent error; no additional resends are attempted; and, an administrator alert is issued.

3.2.2.2 Google Chat Messages

Using the configurations described in Section 3.2.1, *Configuration of DCGA Export Service for Digital Communications*, when Google Chat messages are journaled for a monitored user, the Google **DCGA Export Service** generates a standard email message and transmits its contents and associated metadata as one file, for ingestion by a third-party DCGA platform. Journalling of posted (created and edited) Chat messages is performed by the Google DCGA Export Service according to the following process:

- For each user in a monitored OU or Group participating in the Google Chat thread, a journal copy of the Google Chat content and associated metadata is created when the Chat message is posted or modified. See the table below for details.
    - When a monitored user is added to an existing chat space or Group DM, they will see existing chat history (if available), however, their individual chat participation is monitored and journaled from the point they are added. Note: Monitored users cannot be added to a DM (i.e., a private direct messaging space) once it has started.
- The journal copies of Google Chats are stored in a Google message queue until the next scheduled SMTP export by the Google DCGA Export Service. See Section 3.5, *Record Redundancy*, for additional details.
- Note: Monitored chat messages are subject to organizational policies, such as *Off the Record* policies, which may prevent the capture of certain journaled messages.

The following table defines a Google Chat message by detailing the message contents and associated metadata that are journaled as a fully formed RFC 5322/MIME message. This journal file for each Chat is transmitted to a third-party DCGA platform for ingestion. Note: Google In-Meeting Chat messages are excluded from the DCGA Export Service.

	Elements Archived in the Journaled Google Chat Message
Message header (message metadata)	● The Google Chat message header metadata, including: ○ From, a.k.a. Sender ID of the user posting the message ○ Subject, including space or DM IDs, and if the user count is under 5 users, a list of the involved users; otherwise, a total user count. ○ Direct Message (DM) or group DM ○ Space ID, which is the space name (if the message is in a Chat space) ○ Google Chat ID, a.k.a., Message ID or Thread ID, if the message belongs to a threaded conversation. ○ To: email address of all users (i.e., distribution lists are broken down to individual users), plus the archive address. ○ Message timestamp (created, edited, deleted) ○ Optional headers

	Elements Archived in the Journaled Google Chat Message
Customized message header (message metadata)	● Optional configuration for Chat archiving which allows for the capture of metadata such as MsgID.
Message content and attachments	● Archived content includes: ○ Message, message edits, and message deletions ○ Membership state changes (when users join/leave a Chat space) ○ Message pinned/unpinned ○ Chat Board Resource pinned/unpinned ○ User reaction or removed reaction ○ Google Meet link, if added ○ Links to native Workspace documents stored in Drive. ● Non-native files (e.g., PDF, CSV) can be uploaded from Drive and attached to a Google Chat message body if Chat-File Sharing capabilities are enabled. If Chat-File Sharing is not enabled, links to the non-native shared files are included in the message body. Note: Drive links and Files are journaled separately.
Message Reactions (Emojis)	● Emojis added to a chat are considered reactions and saved as metadata for the associated message. The metadata includes a reference to the source message along with a Unicode representation of the reaction. ● When emojis are removed from a chat, the action is also recorded as metadata for the associated message. Metadata includes a reference to the source message along with a Unicode representation of the deleted reaction.

When planning the process of journaling Google Chat messages using the DCGA Export Service, the regulated entity is responsible for:

- Defining custom headers if required by the DCGA platforms to distinguish between journaled Google Chat and Gmail messages.
- Disallowing use of the Chat App Card, viewing a task, and other interactions that may be visible in Google Chat but are not written to the Chat stream, and therefore are not supported for journaling.
- Disabling *Off the Record* chat capabilities as this organizational policy prevents the journaling of chats.
- Monitoring administrator alerts for journaled messages that fail delivery to the DCGA email address; any Google Chat messages not flagged as a failed delivery were successfully transmitted to the DCGA platform.
    - When delivery fails for a journaled message, the SMTP host returns a temporary error, and the **Gmail service** attempts to resend the message for 8 days. If delivery remains unsuccessful, the SMTP host returns a permanent error; no additional resends are attempted; and, an administrator alert is issued.

3.2.2.3 Google Calendar Event Messages

Using the configurations described in Section 3.2.1, *Configuration of DCGA Export Service for Digital Communications*, when Google Calendar event messages are journaled for a monitored user, the Google **DCGA Export Service** generates a standard email message and transmits its contents and associated metadata as one file, for ingestion by a third-party DCGA platform. Journalling of created, updated or deleted Google Calendar events is performed by the Google DCGA Export Service according to the following process:

- For each user (Google Calendar organizer or recipient) in a monitored OU or Group, a journal copy of the Google Calendar event content and associated metadata is created as an iCalendar (ICS) attachment to an email when a Google Calendar event is created, modified, or deleted, as well as monitored users added as a recipient, via a routing rule. Additionally, event reminders are automatically sent up to 24 hours prior to the start of every event to ensure at least one archive export is created for pre-existing calendar entries for newly-monitored individuals.
  - Routing rules apply when a delegate sends a Google Calendar meeting invitation.
  - Journaled Google Calendar event messages are created for:
    - Single meeting events and recurring meetings with or without an end date.
    - Primary and secondary (i.e., shared or specific-purpose) calendars. Accordingly, if a monitored user has edit access to a secondary calendar, its Google Calendar events will be archived.
  - Note: Gmail messages or Chats sending a meeting link and other methods of bypassing use of Google Calendar invitations, will not be archived as a Google Calendar event message.
- The journal copies of Google Calendar event messages are transmitted via SMTP to the specified DCGA email address, within minutes of the original communication being sent.

The following table defines a Google Calendar event message by detailing the contents and associated metadata that are journaled as an **iCalendar (ICS) file** attached to an email containing the event in RFC 5545 format.

	Elements Archived in the iCalendar (ICS) File attached to the Journaled Message of a Google Calendar Event
Primary properties	● iCalendar (ICS) files contain several components, e.g., VCALENDAR, VEVENT, VTODO, VTIMEZONE, and VALARM. ● The primary properties for an ICS file include: ○ Event ID ○ User email address ○ Event start and end times and associated display time zones ○ Event summary and event description ○ Attachment Title (i.e., name of attached Google Doc) and attachment URL ○ Link to meeting ○ Event creation and last modified timestamps ○ Event location ○ Event Organizer ○ Event invitees (attendees), their responses with any notes ○ Event status (i.e., cancelled or confirmed) ○ Event type (e.g., OOO and Focus time) ○ Joining method (i.e., virtual or meeting room).
Participant lists	● Monitored users are detected, whether they are top-level attendees, indirect recipients, or are named in nested distribution lists and an email message with the attached ICS file is journaled for each monitored user. ● Within the ICS file, only the top-level attendees are listed, which includes the title of the Group distribution list and the membership, as long as the monitored individual (aka "actor") has access to view the members of the Group.

	Elements Archived in the iCalendar (ICS) File attached to the Journaled Message of a Google Calendar Event

Attachments to ICS files	● Attachments can be inserted into an ICS file as:
	  ● Links to native Workspace documents stored in Drive.
	  ○ URL references (links to accessible content).
	  ○ Non-native files (e.g., PDF, CSV), which is embedded in the ICS file text.
	● Post-meeting artifacts (e.g., recordings, transcripts) that are generated at the conclusion of a Meet event are sent back to the associated Calendar event and captured in a change archival export.

Emojis	● Emojis may be embedded in the subject or body of a Google Calendar event. ● The ICS file stores the Unicode code point for each emoji, and the renders it as the corresponding graphic.

When planning the process of journaling Google Calendar event messages using the DCGA Export Service, the regulated entity is responsible for:

- Monitoring administrator alerts for journaled Google Calendar event messages that fail delivery to the DCGA email address. For example, if Spanner snapshots fail, due to a 4-hour processing limitation, notifications that include the live status of the event are generated.

3.3 Google DWT Export Services for Oral Conversations

The DWT Export Service is designed to automate the process of journaling Meet artifacts (Meeting recording, transcript and attendance metadata) for monitored users to the DCGA platform selected by the regulated entity. Note: As identified in Section 1.3, Live Stream Meetings, Meet Calls (formerly Duo) and Meet Legacy Calls are out of scope for this assessment.

It is Cohasset's opinion that the functionality of Google with the DWT Export Service supports the regulated entity in meeting its requirements for oral conversations, when configured and implemented, as described in this section.

3.3.1 Configuration of DWT Export Service for Oral Conversations

The regulated entity is responsible for identifying the users whose oral conversations are required books and records, then designating the monitored users by OU or Group, as described in the following table, which lists the service-specific licensing and configurations required to enable the automated export of Google Meet artifacts (i.e., Meet recordings, transcripts and attendance metadata) for Scheduled and Ad Hoc meetings.

	Configurations required for the Google DWT Export Service for Google Meet artifacts (i.e., Meet recordings, transcripts and attendance metadata)
Licensing	● One of the following Workspace licensing options that support the **automatic meeting artifact** settings is required: Business Plus, Enterprise Standard, Enterprise Plus, Teaching and Learning Upgrade, Education Plus, Enterprise Essentials, or Enterprise Essentials Plus. ● No add-on licensing is required.

	Configurations required for the Google DWT Export Service for Google Meet artifacts (i.e., Meet recordings, transcripts and attendance metadata)
Google Cloud Platform (GCP) Project with Lien	● A GCP Project must be created within the GCP account layer, with appropriate GCS ownership permissions set. ● A *Lien* should be set at the GCP Project-level that is inherited by the Bucket, to prohibit inadvertent Bucket deletion in the event a GCP Project is removed from the account layer of GCP. Note: Cohasset recommends that the creation of Project-level *Liens* be automated within the regulated entity's GCP environment, which provides enforcement of governance policies by preventing administrators with special privileges from inadvertently removing Project-level *Liens* and associated storage Buckets that may contain unexpired required records.
GCS Temporary Storage Bucket	● To prevent deletion of Meet artifacts before export to the DCGA platform, a GCS **Temporary Storage Bucket** is leveraged to temporarily hold Meet artifacts. The Temporary Storage Bucket must be configured as follows: ○ A retention duration (i.e., 30 days is recommended) is applied as the Bucket's retention policy. ○ The Bucket retention policy is locked (lock status set to true, a.k.a., a locked GCS Bucket) to assure the Bucket's retention duration cannot be shortened or removed. ○ Object versioning is disabled for the Bucket. ○ The Bucket is linked to a Domain Wide Takeout (DWT) policy; see row below for details on DWT. ● A Google Cloud Object Storage Lifecycle deletion rule may be set to a value equal to the Bucket retention policy to ensure all temporary artifacts are removed once past their retention period.
Identifying monitored hosts and setting up Group, if needed	● When Meet artifacts are a required record, the **meeting host**[28] (i.e., owner of Meet artifacts) and co-hosts must be monitored, to ensure Meet artifacts are properly exported from the host's Drive to a third-party DCGA platform. ○ Note: Meeting hosts (and co-hosts) can override and thereby block the automated capture of Meet artifacts on a per-meeting basis. Therefore, regulated entities required to keep recordings of certain oral conversations (e.g., ***disciplined firms*** subject to FINRA Rule 3170 Taping Rule and firms required to keep oral communications for one year per the CFTC regulation 17 CFR 1.31), must evaluate whether Google Meet enables sufficient assurance of compliance. ● Meet artifacts are exported via DWT (see next row), when configured for meeting hosts and co-hosts based on the following criteria: ○ Workspace Domain: Meet artifacts are captured for any meeting hosted by a user on the domain. ○ Organization Unit (OU): Meet artifacts are captured when the meeting host is a member of the OU. ○ Group of Workspace Domain users (i.e., a logical set of users created for the purpose of applying specific settings and access controls): Meet artifacts are captured when the meeting host is a member of the Group. When using Groups to designate monitored hosts: ▪ Members of the Group may span multiple OUs. Note: A user can belong to multiple Groups, but to only one OU. ▪ The monitored Group must be assigned a high priority when created, to ensure the appropriate recording settings are applied to each monitored host, since users receive settings from the highest priority Group they are a member of.

[28] Meet artifacts are stored for the primary host, and if configured, for any co-host added in advance of the meeting.

	Configurations required for the Google DWT Export Service for Google Meet artifacts (i.e., Meet recordings, transcripts and attendance metadata)
Domain Wide Takeout (DWT)	● DWT administrators must configure an automated DWT export policy: ○ The DWT export policy must be applied to the monitored meeting hosts and co-hosts, as identified in the preceding row. ○ The GCS Temporary Storage Bucket must be specified as the target export location. ○ The export must be defined as a continuous export, to ensure the export process runs daily to move Meet artifacts from the Meeting host's Drive to the specified Temporary Storage Bucket in GCS. Meet artifacts are copied to the specified GCS Bucket between 24 and 72 hours from creation.
Disabling DWT export of Meet Artifacts	● Administrators can disable the DWT export of future meetings (i.e., already scheduled meetings, as well as those not yet scheduled) by (a) modifying or deleting the DWT export policy or (b) removing users from the OU or Group. Therefore, procedural controls and monitoring of administrative actions are required to scrutinize changes which may result in disabling the export of Meet artifacts for a user or set of users.
Meet Settings that must be enabled, when the associated Meet artifact is a *required record*.	
Recordings with Joining Rule	● Automatic recordings are disabled by default and must be **enabled**. ● The setting for *Host must join before anyone else can join* is disabled by default and must be **enabled**. ○ When this joining rule is enabled, the meeting and recording will start as soon as the meeting host joins.
Transcripts	● Automatic Meeting Transcripts is **enabled** by default and may be **disabled**, if the regulated entity does not need to capture transcripts as required records.
Meet features that must be disabled when the regulated entity determines that the related content is a required record. ● Disabling the feature for the Workspace Domain assures these features are not used in a Meet event. ● When the feature is disabled for only monitored users, non-monitored attendees may utilize the feature during the Meet event, though the monitored attendees cannot view or participate in use of the feature.	
Dial-In access and third-party meeting integrations	● To ensure that only authenticated attendees join meetings, participants must be disallowed from joining via dial-in or third-party meeting integrations, since these participants are not authenticated attendees. ○ Disable the Telephony feature to prevent dial-in access to meetings. ○ Do not configure Gateway Interoperability to prevent third-party meeting integrations (e.g., Zoom meeting joining a Google Meet event).
Gemini	● Gemini prompts and responses may not be captured in the Meet recording or transcript and therefore if Gemini interactions are a required record, this Meet feature must be disabled. ● The Gemini Notes feature requires Gemini to be enabled. By default, Gemini Notes is disabled, but may be enabled for a Group, OU or Workspace Domain. The Gemini-generated meeting notes are stored as a .txt file and managed as a Meet artifact, like the recordings, transcripts and attendance metadata.
In-Meeting Chat	● In-Meeting Chats are captured in a chat log, only when the option is selected by the Meeting host, for the specific meeting. Therefore, if Chat is a required record, this Meet feature must be disabled for the Domain.
Emoji's and Reactions	● Emojis and reactions are displayed only during the meeting and are not captured. Therefore, if emojis and reactions are required records, this Meet feature must be disabled for the Domain.
Q&A	● Questions and answers are displayed during the meeting, and the Q&A Meet artifact captures only the questions. Therefore, if questions and answers are required records, this Meet feature must be disabled for the Domain.
Polls	● Polls is an integrated application that does not generate content captured as a Meet artifact. Therefore, if polls or poll tallies generate a type of required record, the integration with Polls must be disabled for the Domain.
Third-party Integrations	● Third-party integrations do not generate content captured as a Meet artifact. Therefore, if the integrated service generates a type of required record, the integration must be disabled for the Domain.

3.3.2 Record Definition and Export Process

For oral conversations that are required books and records, the following details (1) the process for capturing Meet artifacts, (2) elements captured as part of each artifact, and (3) archive planning considerations.

Using the configurations described in Section 3.3.1, *Configuration of DWT Export Service for Oral Conversations*, Google Meet artifacts are stored for a monitored **meeting host**, rather than for each monitored individual in attendance. The **DWT Export Service** stores the Meet artifacts and makes them available for ingestion by a third-party DCGA platform according to the following process:

- Meet artifacts and associated metadata are automatically written to a monitored host's Drive at the conclusion of the Meet event; see the table below for details on the artifacts captured.
- Copies of the Meet artifacts are exported from Drive within 24 to 72 hours, as long as the meeting host and automated retention and deletion policies have not deleted or moved the Meet artifacts prior to export.
- Note: Procedural controls and monitoring are required to scrutinize actions taken that circumvent the capture of Meet artifacts, such as: (a) Meeting hosts (and co-hosts) taking actions to override and thereby block the automated capture of Meet artifacts on a per-meeting basis (b) Meeting hosts moving the Meet artifacts prior to export.
- The automated DWT export process runs daily to export a copy of all Meet artifacts from the Meeting hosts' Drives.
    - A copy of each Meet artifact and associated metadata is exported to the GCS Temporary Storage Bucket that is identified within the DWT export policy. Note: Based on current DWT functionality, a Meet artifact may be exported to GCS multiple times until the source artifact is removed from the Meeting host's Drive by the Meeting host or via an automated retention and deletion policy.
    - GCS applies integrated immutability and retention controls to the temporary copy of artifacts as they are written to the locked Bucket, according to the configured Bucket policy.
    - GCS APIs are used to export a copy of each Meet artifact and associated metadata from the locked GCS Bucket to a third-party DCGA platform for compliant archival. The third-party DCGA platform is responsible for (a) exporting only new Meet artifacts (i.e., ignoring duplicate artifacts) and (b) normalizing, parsing, and indexing the exported artifacts to enable supervisory activities within their platform.

The following table defines the Meet artifacts that may be captured and exported as a *required record*, if enabled during configuration and not disabled by the meeting hosts.

	Artifacts captured as part of a Meet event
Recording	● Video recordings are captured as MP4 files.
Transcripts	● Meeting transcripts are captured as a .txt file. ○ Note: Closed captions may be enabled separately to display during the meeting but are not captured as part of a transcript or other separate text-based artifact. ○ Only authenticated attendees are identified in the transcript; dial-in or third-party meeting integrations are not identified as authenticated attendees and therefore, should be disabled via configurations.

	Artifacts captured as part of a Meet event
Attendance metadata	● Metadata for each meeting is captured in a separate TXT file and includes: ○ Meeting ID ○ Meeting start and end timestamps ○ Attendee names, IDs and timestamps for joining and/or leaving the meeting

When planning the process of exporting Meet artifacts using a DWT export policy, the regulated entity is responsible for the following:

- The regulated entity must determine what meeting content is considered a required book and record and (a) configure the required features, (b) apply the configurations to hosts of monitored meetings and (b) manage users in monitored Groups or OUs, as appropriate.
- Meet artifacts are not captured for Breakout Room meetings and there is currently no option to administratively disable the Breakout Room feature. Therefore, Cohasset recommends that the use of host-controlled Breakout Rooms be procedurally disallowed with appropriate monitoring.
- Meeting hosts (and co-hosts) can override and thereby block the automated capture of Meet artifacts on a per-meeting basis and Meeting hosts can move the Meet artifacts prior to export. Procedural controls and monitoring are required for both of these actions, which, if taken, circumvent the capture of Meet artifacts.
- The administrator should regularly review export logs to ensure Meet artifacts are successfully exported to (a) the GCS Temporary Storage Bucket and (b) the third-party DCGA platform.

3.4 Record Redundancy

- Google uses erasure coding, which stores coded segments of the record across multiple disks located in different disks, racks, and availability zones (i.e., separate power and network failure domains). In the event of an error, an accurate replica of the full record can be regenerated.
  - Erasure coding applies to Google Drive and temporary storage of files queued for transmission to third-party DCGA platforms.
  - The erasure coded segments are retained for the same time period as the associated file.
- Google calculates and stores checksums to validate data is unchanged and corrects any identified errors.

3.5 Audit Log and Administrative Alerts

- The following Google Audit Logs are available to facilitate review and troubleshooting of the Workspace environment:
  - Admin Log - captures administrative actions taken to configure Google Export Service.
    - Log entries include action taken, email address of user who performed action and their OU, timestamp of action, message ID, old value, and new value.
  - Gmail Log – captures user and administrator actions taken relative to Gmail.

  - Log entries include, but are not limited to, message ID, action taken (e.g., send, view, download attachment, delete), To/From, delegate (if any), subject, timestamp of action, spam classification and reason, malware category, as well as information related to a user interacting with a message or its links and attachments.
- Chat Log – captures user and administrator actions taken relative to Chat.
  - Log entries include, but are not limited to, actor (email address), actor's Group name and OU, attachment name and URL, conversation type, event timestamp, message ID, chat history on/off, recipients (if an invite is sent, a user is blocked, a user is added to a space or room, a DM is sent, modified or deleted), etc.
- Calendar Log – captures user and administrator actions taken relative to Calendar.
  - Log entries include, but are not limited to, actor (email address of user), actor's Group name and OU, calendar ID, timestamp, event (e.g., title change, guests added or removed, event deleted), with old value and new value, etc.
- Meet Log – captures user and administrator actions taken relative to Meet.
  - Log entries include, but are not limited to, actor (email or phone number of user), actor's Group name or OU, meeting code, event, event timestamp, attendees of a meeting, etc.

- Log entries are retained for a maximum of six months.
- Log entries can be reviewed, using a variety of filtering options, using the Audit and Investigations menu.
- Administrative alerts can be set up based on log event data, using reporting tools or activity rules.
- Audit log entries can be exported; examples include:
  - Exporting to Google BigQuery on the Google Cloud Platform for longer term storage and further analytics.
  - Exporting up to a maximum of 100,000 rows to Google Sheets or to a CSV file for longer term storage or ingestion by a security information and event management tool.

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

This section contains a summary assessment of the functionality of Workspace, as described in Section 1.3, *Workspace Overview and Assessment Scope*, in comparison to CFTC electronic regulatory record requirements. Specifically, this section associates the features described in Section 2, *Assessment of Google Workspace with AODocs Compliance Archive for 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.*[29] [emphasis added]

In Section 2 of this report, Cohasset assesses Workspace, with AODocs Compliance Archive, a highly restrictive option that applies integrated controls to (a) prevent overwriting and modifying 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 assessed functionality. The first column enumerates the CFTC regulation. The second column provides Cohasset's analysis and opinion regarding the ability of Workspace, relative to these requirements.

[29] 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[30] with time-based retention periods, are met by the functionality of Workspace, with AODocs Compliance Archive. 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 2.8, *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] Workspace with AODocs Compliance Archive retains immutable metadata (e.g., GCS Global Identifier, Retention Expiration Time and GCS storage 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, an extensive index is retained for the same time period as the associated record, to facilitate search and retrieval. See Sections 2.4, 2.8 and 2.9 for Workspace capabilities related to retaining information needed to search and locate the records. Further, Workspace in conjunction with the Retention Audit Logs 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*.

[30] 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 Workspace capabilities described in Section 2.5, *Record Redundancy*, including methods for a persistent duplicate copy or alternate source to reestablish the records and associated system metadata, 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 Workspace storage classes are designed for 11-nines of durability, using erasure coding to store data pieces redundantly across different disks, racks, and availability zones (i.e., separate power and network failure domains). In the event of an error, an accurate replica of the full record can be regenerated.
(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 Workspace with AODocs Compliance Archive 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*

5 • Conclusions

Cohasset assessed the functionality of Google[31] with AODocs Compliance Archive 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 with AODocs Compliance Archive, when properly configured, has the following functionality, which meets the regulatory requirements in SEC Rules 17a-4(f)(2) and 18a-6(e)(2):

- Retains records and associated metadata in a non-rewriteable, non-erasable format for time-based retention periods, when *GCS Bucket Lock* retention controls are applied.
- Allows a legal hold to be applied to a record subject to preservation requirements, by setting both the AODocs *On Hold* flag and the GCS *Temporary Hold* flag, which retain the record as immutable and prohibits deletion or overwrites until both settings are removed.
- Prohibits deletion of a record and its immutable metadata until the applied *Target Destruction Date* is in the past.
- Verifies the accuracy and quality of the recording process through the use of checksums and post-recording validation processes, in addition to the inherent capabilities of advanced storage recording technology.
- Regenerates an accurate replica of the record and properties (indexes and metadata) from erasure coded data should an error occur in one segment of the data or an availability problem be encountered in any one of the power or network domain locations. Additionally, provides the ability to restore a record and properties (indexes and metadata) from a persistent duplicate copy retained on GCS Coldline storage.
- Provides the capacity and tools to (a) list records and (b) download selected records and associated properties (indexes and metadata) for a browser and/or other local tool to render a human-readable image.

Additionally, Google with AODocs Compliance Archive 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 metadata related to inputting each record and downloading this metadata 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.

Cohasset also correlated the assessed capabilities of AODocs to the principles-based electronic records requirements in CFTC Rule 1.31(c)-(d).

[31] Google functionality includes (a) Google Workspace to authenticate users and provide collaboration, (b) Google Drive to store working copies of native content (i.e., Google Docs, Sheets and Slides) and non-native content (i.e., other Google Drive files, such as PDFs, images and video), (c) Google Cloud Storage for final records, and (d) other Google services.

Accordingly, Cohasset concludes that Google with AODocs Compliance Archive, 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).

Cohasset also concludes that Google Export Services, specifically the DCGA Export Service and the DWT Export Service, supports compliance archiving of digital communications, as described in Section 3, *Assessment of Google Compliance Archiving Support for Digital Communications and Oral Conversations*, by automating the process of exporting journaled messages to third-party platforms to preserve, monitor, supervise, and manage digital communications.

Appendix A • Overview of Relevant Electronic Records Requirements

This section establishes the context for the regulatory requirements that are the subject of Cohasset's assessment in Section 2, Assessment of Google Workspace with AODocs Compliance Archive for Compliance with SEC Rules 17a 4(f) and 18a 6(e) *and Section 4,* Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d), *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[32] 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.*[33] [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.*[34] [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.

---

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

[33] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66428.

[34] 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.*[35] [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.*[36] [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."*[37] [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****[38] [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).

35 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.
36 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.
37 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66418.
38 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.*[39] [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.*[40] [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.*[41] [emphasis added]

See Section 2, *Assessment of Google Workspace with AODocs Compliance Archive for 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 Workspace 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).[42]

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.*

---

39 2003 Interpretative Release, 68 FR 25282.

40 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).

41 2003 Interpretative Release, 68 FR 25283.

42 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.*[43] [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 Workspace in relation to each requirement, see Section 4, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*.

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

Appendix B • Overview of Relevant Requirements for Digital Communications and Oral Conversations

This section contains excerpts of the certain regulatory requirements pertinent to digital communications in the financial services industry, which is the subject of Cohasset's assessment in Section 3, Assessment of Google Compliance Archiving Support for Digital Communications and Oral Conversations.

B.1 Overview of SEC Digital Communications Requirements for Broker-Dealers, Securities-Based Swap Dealers and Major Security-Based Swap Participants

B.1.1 SEC Requirements for Communications in Rule 17a-4(b)

In 17 CFR § 240.17a-4(b) for the securities broker-dealer industry, the SEC mandates retention of communications:

> *(b) Every member, broker or dealer subject to § 240.17a-3 must preserve for a period of not less than three years, the first two years in an easily accessible place:*
>
> *****
>
> *(4) Originals of all communications received and copies of all communications sent (and any approvals thereof) by the member, broker or dealer (including inter-office memoranda and communications) relating to its business as such, including all communications which are subject to rules of a self-regulatory organization of which the member, broker or dealer is a member regarding communications with the public. As used in this paragraph (b)(4), the term communications includes sales scripts and recordings of telephone calls required to be maintained pursuant to section 15F(g)(1) of the Act (15 U.S.C. 78o-10(g)(1)).*
>
> ***** [emphasis added]

B.1.2 SEC Requirements for Communications in Rule 18a-6(b)

In 17 CFR § 240.18a-6(b) for security-based swap dealers and major security-based swap participants, the SEC mandates retention of communications:

> *(b) (1) Every security-based swap dealer and major security-based swap participant for which there is no prudential regulator must preserve for a period of not less than three years, the first two years in an easily accessible place:*
>
> *****
>
> *(iv) Originals of all communications received and copies of all communications sent (and any approvals thereof) by the security-based swap dealer or major security-based swap participant (including inter-office memoranda and communications) relating to its business as such. As used in this paragraph (b)(1)(iv), the term "communications" includes sales scripts and recordings of telephone calls required to be maintained pursuant to section 15F(g)(1) of the Act (15 U.S.C. 78o-10(g)(1)).*
>
> ***** [emphasis added]

B.1.3 SEC Requirements for Communications in 15 U.S.C. 78o-10(g)

Both Rules 17a-4(b) and Rule 18a-6(b) reference the requirements of 15 U.S.C. 78o-10(g), which applies to registered security-based swap dealers and major security-based swap participants and stipulates:

(g) daily trading records

(1) In general

Each registered security-based swap dealer and major security-based swap participant shall maintain daily trading records of the security-based swaps of the registered security-based swap dealer and major security-based swap participant and all related records (including related cash or forward transactions) and recorded communications, including electronic mail, instant messages, and recordings of telephone calls, for such period as may be required by the Commission by rule or regulation.

***** [emphasis added]

B.2 Overview of FINRA Requirements for Digital Communications and Oral Conversations

B.2.1 FINRA Requirements for Communications in Rule 3110, *Supervision*

Financial Industry Regulatory Authority (FINRA) Rule 3110(b), *Supervision*, requires supervisory review of correspondence and internal communications. Specifically, paragraph (b) stipulates:

(b) Written Procedures

(1) General Requirements

Each member shall establish, maintain, and enforce written procedures to supervise the types of business in which it engages and the activities of its associated persons that are reasonably designed to achieve compliance with applicable securities laws and regulations, and with applicable FINRA rules.

*****

(4) Review of Correspondence and Internal Communications

The supervisory procedures required by this paragraph (b) shall include procedures for the review of incoming and outgoing written (including electronic) correspondence and internal communications relating to the member's investment banking or securities business. The supervisory procedures must be appropriate for the member's business, size, structure, and customers. The supervisory procedures must require the member's review of:

(A) incoming and outgoing written (including electronic) correspondence to properly identify and handle in accordance with firm procedures, customer complaints, instructions, funds and securities, and communications that are of a subject matter that require review under FINRA rules and federal securities laws.

(B) internal communications to properly identify those communications that are of a subject matter that require review under FINRA rules and federal securities laws.

Reviews of correspondence and internal communications must be conducted by a registered principal and must be evidenced in writing, either electronically or on paper.

***** [emphasis added]

B.2.2 FINRA Requirements for Communications in Rule 2210, *Communications with the Public*

FINRA Rule 2210, *Communications with the Public*, categorizes communications into retail communications, correspondence, and institutional communications, and sets standards for supervisory review and recordkeeping.

(a) Definitions

For purposes of this Rule and any interpretation thereof:

(1) "Communications" consist of correspondence, retail communications and institutional communications.

(2) "Correspondence" means any written (including electronic) communication that is distributed or made available to 25 or fewer retail investors within any 30 calendar-day period.

(3) "Institutional communication" means any written (including electronic) communication that is distributed or made available only to institutional investors, but does not include a member's internal communications.

*****

(5) "Retail communication" means any written (including electronic) communication that is distributed or made available to more than 25 retail investors within any 30 calendar-day period.

*****

(b) Approval, Review and Recordkeeping

(1) Retail Communications

(A) An appropriately qualified registered principal of the member must approve each retail communication before the earlier of its use or filing with FINRA's Advertising Regulation Department ("Department").

*****

(2) Correspondence

All correspondence is subject to the supervision and review requirements of Rules 3110(b) and 3110.06 through .09.

(3) Institutional Communications

Each member shall establish written procedures that are appropriate to its business, size, structure, and customers for the review by an appropriately qualified registered principal of institutional communications used by the member and its associated persons. Such procedures must be reasonably designed to ensure that institutional communications comply with applicable standards. When such procedures do not require review of all institutional communications prior to first use or distribution, they must include provision for the education and training of associated persons as to the firm's procedures governing institutional communications, documentation of such education and training, and surveillance and follow-up to ensure that such procedures are implemented and adhered to. Evidence that these supervisory procedures have been implemented and carried out must be maintained and made available to FINRA upon request.

(4) Recordkeeping

(A) Members must maintain all retail communications and institutional communications for the retention period required by SEA Rule 17a-4(b) and in a format and media that comply with SEA Rule 17a-4. The records must include:

(i) a copy of the communication and the dates of first and (if applicable) last use of such communication;

(ii) the name of any registered principal who approved the communication and the date that approval was given;

(iii) in the case of a retail communication or an institutional communication that is not approved prior to first use by a registered principal, the name of the person who prepared or distributed the communication;

(iv) information concerning the source of any statistical table, chart, graph or other illustration used in the communication;

(v) for any retail communication for which principal approval is not required pursuant to paragraph (b)(1)(C), the name of the member that filed the retail communication with the Department, and a copy of the corresponding review letter from the Department; and

(vi) for any retail communication that includes or incorporates a performance ranking or performance comparison of a registered investment company, a copy of the ranking or performance used in the retail communication.

(B) Members must maintain all correspondence in accordance with the record-keeping requirements of Rules 3110.09 and 4511. [emphasis added]

Supplementary Material pertaining to 3110.06 through .09 stipulates:

.06 Risk-based Review of Correspondence and Internal Communications. By employing risk-based principles, a member must decide the extent to which additional policies and procedures for the review of:

(a) incoming and outgoing written (including electronic) correspondence that fall outside of the subject matters listed in Rule 3110(b)(4) are necessary for its business and structure. If a member's procedures do not require that all correspondence be reviewed before use or distribution, the procedures must provide for:

(1) the education and training of associated persons regarding the firm's procedures governing correspondence;

(2) the documentation of such education and training; and

(3) surveillance and follow-up to ensure that such procedures are implemented and followed.

(b) internal communications that are not of a subject matter that require review under FINRA rules and federal securities laws are necessary for its business and structure.

.07 Evidence of Review of Correspondence and Internal Communications. The evidence of review required in Rule 3110(b)(4) must be chronicled either electronically or on paper and must clearly identify the reviewer, the internal communication or correspondence that was reviewed, the date of review, and the actions taken by the member as a result of any significant regulatory issues identified during the review. Merely opening a communication is not sufficient review.

.08 Delegation of Correspondence and Internal Communication Review Functions. In the course of the supervision and review of correspondence and internal communications required by Rule 3110(b)(4), a supervisor/principal may delegate certain functions to persons who need not be registered. However, the supervisor/principal remains ultimately responsible for the performance of all necessary supervisory reviews, irrespective of whether he or she delegates functions related to the review. Accordingly, supervisors/principals must take reasonable and appropriate action to ensure delegated functions are properly executed and should evidence performance of their procedures sufficiently to demonstrate overall supervisory control.

.09 Retention of Correspondence and Internal Communications. Each member shall retain the internal communications and correspondence of associated persons relating to the member's investment banking or securities business for the period of time and accessibility specified in SEA Rule 17a-4(b). The names of the persons who prepared outgoing correspondence and who reviewed the correspondence shall be ascertainable from the retained records, and the retained records shall be readily available to FINRA, upon request. [emphasis added]

B.3.1 FINRA Requirements for Tape Recording Telephone Conversations in Rule 3170

FINRA Rule 3170, *Tape Recording of Registered Persons by Certain Firms*, is intended to enhance oversight and surveillance of firms hiring registered representatives with a history of compliance issues. The Rule mandates that certain firms record and retain telephone conversations between their registered persons and customers, review those recordings, and report their findings to FINRA.

Guidance on FINRA Rule 3170, *Tape Recording of Registered Persons by Certain Firms*, stipulates:

> *FINRA Rule 3170 (Tape Recording of Registered Persons by Certain Firms)—commonly referred to as the "Taping Rule"—requires certain firms to install taping systems to record all telephone conversations between their registered persons and existing and potential customers, review those recordings and file reports with FINRA.*
>
> *The Taping Rule is designed to prevent fraudulent and improper practices in the sale or marketing of financial products and behavior that may otherwise cause customer harm. As such, the rule applies to member firms with a significant number of registered persons that previously worked for firms that have been expelled from FINRA membership or have had their registrations revoked for inappropriate sales practices. Firms that become subject to these requirements are called "taping firms."*
>
> *Taping firms must establish, enforce and maintain special written supervisory procedures, tape record conversations for a period of three years, at a minimum, and review those recordings for compliance purposes. Taping firms must also provide quarterly reports to FINRA on the taping firm's supervision of its registered persons' telemarketing activities and retain the tape recordings consistent with the retention requirements in Rule 3170.* [emphasis added]

B.3 Overview of SEC Digital Communications Requirements for Investment Advisors

B.3.1 SEC Requirements for Communications in Rule 204-2(a)

In 17 CFR §§ 275.204-2(a) for investment advisors, the SEC mandates preservation of certain types of written communications, including communications related to recommendations, transactions, and performance.

> *(a) Every investment adviser registered or required to be registered under section 203 of the Act (15 U.S.C. 80b–3) shall make and KEEP true, accurate and current the following books and RECORDS relating to its investment advisory business;*
>
> *****
>
> *(7) Originals of all written communications received and copies of all written communications sent by such investment adviser relating to:*
>
> *(i) Any recommendation made or proposed to be made and any advice given or proposed to be given;*
>
> *(ii) Any receipt, disbursement or delivery of funds or securities;*
>
> *(iii) The placing or execution of any order to purchase or sell any security; and, for any transaction that is subject to the requirements of § 240.15c6-2(a) of this chapter, each confirmation received, and any allocation and each affirmation sent or received, with a date and time stamp for each allocation and affirmation that indicates when the allocation and affirmation was sent or received;*
>
> *(iv) Predecessor performance (as defined in § 275.206(4)-1(e)(12) of this chapter) and the performance or rate of return of any or all managed accounts, portfolios (as defined in § 275.206(4)-1(e)(11) of this chapter), or securities recommendations; Provided, however:*
>
> *(A) That the investment adviser shall not be required to keep any unsolicited market letters and other similar communications of general public distribution not prepared by or for the investment adviser; and*

(B) That if the investment adviser sends any notice, circular, or other advertisement (as defined in § 275.206(4)-1(e)(1) of this chapter) offering any report, analysis, publication or other investment advisory service to more than ten persons, the investment adviser shall not be required to keep a record of the names and addresses of the persons to whom it was sent; except that if such notice, circular, or advertisement is distributed to persons named on any list, the investment adviser shall retain with the copy of such notice, circular, or advertisement a memorandum describing the list and the source thereof.

*****[emphasis added]

B.3.2 SEC Requirements for Communications in Rule 206(4)-7

In 17 CFR §§ 275.206(4)-7 for investment advisors, the SEC mandates compliance procedures and practices, which is interpreted as including supervision and review of communications with clients and the public to ensure compliance and prevent fraud and misleading statements.

If you are an investment adviser registered or required to be registered under section 203 of the Investment Advisers Act of 1940 (15 U.S.C. 80b-3), it shall be unlawful within the meaning of section 206 of the Act (15 U.S.C. 80b-6) for you to provide investment advice to clients unless you:

(a) Policies and procedures. Adopt and implement written policies and procedures reasonably designed to prevent violation, by you and your supervised persons, of the Act and the rules that the Commission has adopted under the Act;

(b) Annual review. Review, no less frequently than annually, the adequacy of the policies and procedures established pursuant to this section and the effectiveness of their implementation; and

(c) Chief compliance officer. Designate an individual (who is a supervised person) responsible for administering the policies and procedures that you adopt under paragraph (a) of this section. [emphasis added]

B.3.3 SEC Media Requirements in Rule 204-2(g)

In 17 CFR §§ 275.204-2(g) for investment advisors, the SEC defines requirements for use of electronic storage to preserve required books and records. These requirements are considered to be less-restrictive than the requirements of SEC Rule 17a-4(f) for broker-dealers and SEC Rule 18a-6(e) for security-based swap dealers and major security-based swap participants.

(g) Micrographic and electronic storage permitted —

*****

(2) General requirements. The investment adviser must:

(i) Arrange and index the records in a way that permits easy location, access, and retrieval of any particular record;

(ii) Provide promptly any of the following that the Commission (by its examiners or other representatives) may request:

(A) A legible, true, and complete copy of the record in the medium and format in which it is stored;

(B) A legible, true, and complete printout of the record; and

(C) Means to access, view, and print the records; and

(iii) Separately store, for the time required for preservation of the original record, a duplicate copy of the record on any medium allowed by this section.

(3) Special requirements for electronic storage media. In the case of records on electronic storage media, the investment adviser must establish and maintain procedures:

(i) To maintain and preserve the records, so as to reasonably safeguard them from loss, alteration, or destruction;

(ii) To limit access to the records to properly authorized personnel and the Commission (including its examiners and other representatives); and

(iii) To reasonably ensure that any reproduction of a non-electronic original record on electronic storage media is complete, true, and legible when retrieved. [emphasis added]

B.4 Overview of CFTC Digital Communications Requirements

B.4.1 CFTC Requirements for Oral Communications in Rule 1.31

In 17 CFR 1.31, the Commodity Futures Trading Commission (CFTC) specifies recordkeeping requirements, including the retention and production of records, which stipulates the *form and manner of retention* (i.e., format and media requirements), which are addressed in Section 4, *Summary of Assessment of Compliance with CFTC Rule 1.31(c)-(d)*.

The definitions in paragraph (a) of Rule 1.31 stipulates that "Regulatory records" means all books and records required to be kept by the Act or Commission regulations, further, paragraph (b) sets a general fixed 5-year retention period and explicitly sets a 1-year retention period for required oral communications.

(a) 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.

(b) 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]

B.4.2 CFTC Requirements for Communications in Rule 1.35(a)

In 17 CFR 1.35(a) requires retention of records of commodity interest and related cash or forward transactions, including oral and written communications provided or received by telephone, voicemail, facsimile, instant messaging, chat rooms, electronic mail, mobile device, or other digital or electronic media.

> *(a) Futures commission merchants, retail foreign exchange dealers, introducing brokers, and members of designated contract markets or swap execution facilities —*
>
> *(1) Futures commission merchants, retail foreign exchange dealers, and certain introducing brokers. Each futures commission merchant, retail foreign exchange dealer, and introducing broker that has generated over the preceding three years more than $5 million in aggregate gross revenues from its activities as an introducing broker, shall:*
>
> *(i) Keep full, complete, and systematic records (including all pertinent data and memoranda) of all transactions relating to its business of dealing in commodity interests and related cash or forward transactions, which shall include all orders (filled, unfilled, or canceled), trading cards, signature cards, street books, journals, ledgers, canceled checks, copies of confirmations, copies of statements of purchase and sale, and all other records, which have been prepared in the course of its business of dealing in commodity interests and related cash or forward transactions (for purposes of this section, all records described in this paragraph (a)(1)(i) are referred to as "commodity interest and related records");*
>
> *(ii) If such person is a member of a designated contract market or swap execution facility, retain and produce for inspection all documents on which trade information is originally recorded, whether or not such documents must be prepared pursuant to the rules or regulations of either the Commission, the designated contract market or the swap execution facility (for purposes of this section, all records described in this paragraph (a)(1)(ii) are referred to as "original source documents," and, together with commodity interest and related records, "transaction records"); and*
>
> *(iii) Keep all oral and written communications provided or received concerning quotes, solicitations, bids, offers, instructions, trading, and prices that lead to the execution of a transaction in a commodity interest and any related cash or forward transactions (but not oral communications that lead solely to the execution of a related cash or forward transaction), whether transmitted by telephone, voicemail, facsimile, instant messaging, chat rooms, electronic mail, mobile device, or other digital or electronic media (for purposes of this section, all communications described in this paragraph (a)(1)(iii) are referred to as "oral pre-trade communications" if transmitted orally or as "written pre-trade communications" if transmitted in writing, and all such communications are referred to collectively as "pre-trade communications").*
>
> ***** [emphasis added]

Appendix C • Cloud Provider Undertaking

C.1 Compliance Requirement

Separate from the electronic recordkeeping system requirements described in Section 2, *Assessment of Google Workspace with AODocs Compliance Archive for 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

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]

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.[44] [emphasis added]

C.2 Google Undertaking Process

- The undertaking requires actions be taken by both parties:
  1. The regulated entity affirms, in writing, it:
     - Is subject to SEC Rules 17a-3, 17a-4, 18a-5 or 18a-6 governing the maintenance and preservation of certain records,
     - Has independent access to the records maintained on Workspace, and
     - Consents to Google fulfilling the obligations set forth in this undertaking.
  2. Google:
     - Acknowledges that the records are the property of the regulated entity,
     - For the duration of the undertaking, agrees to facilitate within its ability, and not impede or prevent, the examination, access, download, or transfer of the records by a regulatory or trustee, as permitted under the law, and
     - Prepares the undertaking, utilizing the explicit language in the Rule, then provides the undertaking to the regulated entity.
- IMPORTANT NOTE: While Google provides this undertaking, as required by the SEC, the regulated entity is not relieved from its responsibility to prepare and maintain required records.

C.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 Workspace, (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, and (f) submitting the undertaking to the SEC, as required.

[44] 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.