Cohasset Associates

Wasabi Hot Cloud Storage

COMPLIANCE ASSESSMENT

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

Abstract

Wasabi Hot Cloud Storage is a global object storage solution designed for compatibility with the Amazon Simple Storage Service (S3) application programming interface (API). The Wasabi Hot Cloud Storage environment is architected as a single tier of high-performing, highly-scalable primary storage that is also suitable for use as secondary, archival storage.

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

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

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

COHASSET'S INDUSTRY INSIGHT AND EXPERIENCE

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

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

May 2023

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

+1.312.527.1550 | www.cohasset.com

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 Wasabi Hot Cloud Storage and the assessment scope.*

1.1 Overview of the Regulatory Requirements

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

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

On October 12, 2022, the U.S. Securities and Exchange Commission (SEC) adopted amendments to 17 CFR § 240.17a-4 (SEC Rule 17a-4) and 17 CFR § 240.18a-6 (SEC Rule 18a-6), which define explicit requirements for electronic storage systems.

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

For additional information, refer to Section 2, *Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e)*, and Section 5.1, *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 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*, and Section 5.3, *Overview of CFTC Rule 1.31(c)-(d) Electronic Regulatory Records Requirements*.

1.2 Purpose and Approach

To obtain an independent and objective assessment of the compliance capabilities of Wasabi Hot Cloud Storage for preserving regulated electronic records, Wasabi 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.

Wasabi engaged Cohasset to:

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

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

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

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

1.3 Wasabi Hot Cloud Storage Overview and Assessment Scope

1.3.1 Wasabi Hot Cloud Storage Overview

Wasabi Hot Cloud Storage is a global object[4] storage solution designed by Wasabi to be compatible with the Amazon Simple Storage Service (S3) application programming interface (API). The Wasabi Hot Cloud Storage environment is architected as a single tier of high-performing, highly-scalable primary storage that is also suitable for use as secondary, or "cold," storage (i.e., data that is accessed less frequently, such as backups and archives).

Wasabi Hot Cloud Storage infrastructure is co-located in thirteen top-tier data centers worldwide. Regulated entities must select the region(s) to be utilized for data storage. Access to the storage regions can be established directly from the internet, over a private network connection, or via a Wasabi Ball Transfer Appliance.

The logical storage architecture of the Wasabi Hot Cloud Storage environment is depicted in figure 1 and described, below:

- A single **Customer Account** ID is assigned to the regulated entity and provides all-inclusive access to Wasabi Hot Cloud Storage services.
- Individual **versions** of records, including associated metadata, are stored in logical containers called **Buckets.** While Wasabi Hot Cloud Storage utilizes a flat storage structure, it supports an optional foldering concept as a means to further organize and restrict access to stored objects. Up to 10,000 Buckets may exist within a given account, each configured according to the type of objects to be stored (i.e., regulated or non-regulated objects).

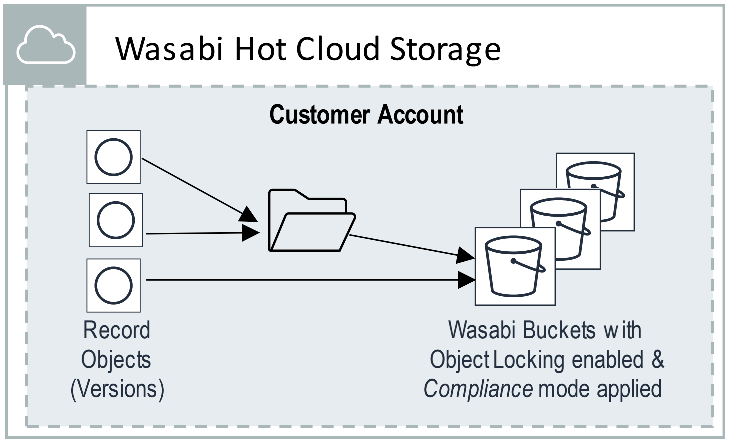
Wasabi Hot Cloud Storage
Customer Account
Record Objects (Versions)
Wasabi Buckets with Object Locking enabled & *Compliance* mode applied

Figure 1: Logical Storage Architecture

- Buckets intended to store required records must be configured with (a) the ***Object Locking*** feature and (b) object versioning enabled. When the *Object Locking* mode for a record is set to ***Compliance*** and a Retain Until Date is applied, integrated controls prevent the record, including its associated metadata, from being modified, overwritten, or deleted until the applied Retain Until Date has expired and any Legal Holds have been removed.

[4] The SEC use the phrase *books and records* to describe information that must be retained for regulatory compliance. Cohasset uses the term *record* (versus object, file or data) to consistently recognize that the content is required for regulatory compliance.

1.3.2 Assessment Scope

The scope of this assessment is focused specifically on the compliance-related capabilities of Wasabi Hot Cloud Storage to meet the non-rewriteable, non-erasable storage requirements of SEC Rule 17a-4(f), when (a) the *Object Locking* feature and object versioning are enabled on the Bucket, (b) *Object Locking* mode for regulated objects is set to *Compliance*, and (c) appropriate Retain Until Dates are applied.

NOTES:

- Excluded from this assessment are (a) the Wasabi Ball Transfer Appliance, utilized for large-scale data transfers in environments with lower connection speeds, (b) other Wasabi storage capabilities, such as the Wasabi Compliance (Bucket-level) feature, and (c) Wasabi Cloud Sync Manager (WCSM), utilized for replication of objects.
- Software as a Service solutions, not managed by Wasabi, are excluded from this report.

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

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

For each of the compliance requirements 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 name their respective regulations and regulators and include semantic differences.
- ***Compliance Assessment*** – Summary statement assessing compliance of Wasabi Hot Cloud Storage
- ***Wasabi Hot Cloud Storage Capabilities*** – Description of assessed functionality
- ***Additional Considerations*** – Additional clarification related to meeting the specific requirement

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

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

> *[L]ike the existing WORM requirement, [the audit-trail requirement] sets forth a specific and testable outcome that the electronic recordkeeping system must achieve: the ability to access and produce modified or deleted records in their original form.*[5] [emphasis added]

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

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

2.1.2 Compliance Assessment

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

For enhanced control, a business-purpose recordkeeping system may store the complete time-stamped audit-trail on Wasabi Hot Cloud Storage, with the features and controls described in Sections 2.2 through 2.6 of this report.

Reminder: This audit-trail requirement is an alternative to the non-rewriteable, non-erasable record format requirement (i.e., write-once, read-many or WORM requirement), which is addressed 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 Audit-Trail*.

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

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

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

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

> *a process of integrated software and hardware codes and clarified that "a software solution that prevents the overwriting, erasing, or otherwise altering of a record during its required retention period would meet the requirements of the rule."*
> *****
> *In 2001, the Commission issued guidance that Rule 17a-4(f) was consistent with the ESIGN Act. The final amendments to Rule 17a-4(f) do not alter the rule in a way that would change this guidance.*[7] [emphasis added]

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

> *[A] broker-dealer must take appropriate steps to ensure that records are not deleted during periods when the regulatory retention period has lapsed but other legal requirements mandate that the records continue to be maintained, and the broker-dealer's storage system must allow records to be retained beyond the retentions periods specified in Commission rules.*[8] [emphasis added]

2.2.2 Compliance Assessment

It is Cohasset's opinion that the functionality of Wasabi Hot Cloud Storage, with the *Object Locking* feature applied in *Compliance* mode, meets this SEC requirement to retain records in non-rewriteable, non-erasable format for the applied time-based[9] retention periods and legal holds, when (a) properly configured, as described in Section 2.2.3, and (b) the considerations described in Section 2.2.4 are satisfied.

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

2.2.3 Wasabi Hot Cloud Storage Capabilities

This section describes the functionality of Wasabi Hot Cloud Storage that directly pertains to this SEC requirement for preserving electronic books and records as non-rewriteable, non-erasable for the required retention period and any applied legal holds.

2.2.3.1 Overview

- Records are transmitted to the Wasabi Hot Cloud Storage environment via (a) Amazon S3-compatible Application Programming Interface (API) commands or (b) upload capabilities (e.g., drag and drop, browse and upload) provided on the Wasabi Management Console, and stored in logical Buckets.
- Retention controls are applied to records during the recording process, based upon either (a) retention controls transmitted with the object or (b) default values, if configured for the target storage Bucket.
- To meet the non-rewriteable, non-erasable requirements of SEC Rule 17a-4(f), a record requiring time-based retention must:
  - be stored in a Bucket that has both (1) versioning and (2) the *Object Locking* feature enabled,

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

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

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

- have an *Object Locking* mode of *Compliance* set for the record,
- have an appropriate Retain Until Date applied to the record, and
- optionally, a Legal Hold flag (Y) may be set which overrides deletion eligibility based on the Retain Until Date and preserves the record until the Legal Hold flag is removed (N or Null).

▶ *When the above conditions are met, Wasabi Hot Cloud Storage applies the following stringent integrated controls:*

- The record, including key system metadata, cannot be modified, overwritten, or deleted by system users (via Wasabi management console, command line interface (CLI) or API) until the applied Retain Until Date has expired and any Legal Hold flag is removed.
- *Compliance* mode controls cannot be removed from the record.
- The applied Retain Until Date cannot be shortened, only extended if necessary.
- The folder (if utilized) containing the locked record cannot be deleted or moved to another Bucket.
- The Bucket containing the record cannot be deleted.

2.2.3.2 Bucket and Identity Access Management (IAM) Configurations

▶ For any Bucket intended to retain required records, the following two configurations must be done *at the time of Bucket creation*:

1. Versioning must be enabled for the Bucket, which results in the creation of a separate record each time an object is modified or overwritten.
2. The *Object Locking* feature must be enabled to prevent objects from being deleted for a fixed amount of time. Once enabled for a Bucket, (a) the *Object Locking* feature cannot be removed, (b) versioning cannot be disabled, (c) the Bucket name cannot be changed, and (d) the Bucket cannot be deleted if it contains any locked records.

▶ Optionally, a pair of default values may be configured for the Bucket. When configured, these default values automatically apply to any record[10] that is either transmitted without explicit retention controls or uploaded into the target Bucket via the Wasabi Management Console:

- The *Object Locking* mode may be set to *Governance* or *Compliance*, **however, only *Compliance* mode allows required records to be stored in compliance with the non-rewriteable, non-erasable requirements of SEC Rule 17a-4(f)** by preventing any user from removing then reducing the applied retention period.
- A retention period (i.e., retention duration) specified in terms of the number of days, weeks, months, or years. The default retention period value is added to the storage date/time to calculate a Retain Until Date which is stored with the record.

[10] Each version of an object is managed as a separate record with its own Object Locking mode and Retain Until Date.

Default values for a Bucket may be modified and/or removed at any time. Updated default values apply day-forward to new records being stored and have no impact to records previously stored.

- While some IAM policies are required and enabled by default (e.g., Administrator Access for the root user), additional IAM policies may be configured to grant appropriate privileges for using *Object Locking* mode, Legal Holds, and Minimum and Maximum (Min/Max) allowable retention values.
  - Once set, Min/Max values serve as guardrails; a Retain Until Date transmitted with a record must fall within the allowable range for that user, otherwise the recording process fails and an error message is issued.
  - If a record is transmitted without retention controls or uploaded into a Bucket via the Wasabi Management Console, and the default Bucket values fall outside of the allowed Min/Max range in the IAM policy for that user, the recording process fails and an error message is issued.
  - Min/Max values defined in a policy may be changed at any time, however, new values apply day-forward as new records are stored.

2.2.3.3 Records, Retention Controls and Legal Holds

- A record is comprised of the following:
  - The content of the object,
  - *Immutable* metadata, including Object Key (Bucket name, folder name, filename), Version ID, creation/storage date/time, and *Object Locking* mode (the mode attribute is immutably retained only when set to *Compliance*), and
  - *Mutable* metadata, including Retain Until Date (may be extended) and Legal Hold (may change between Y/N/Null).
- Each version of an object is considered a separate record and must, therefore, have its own applied *Object Locking* mode, Retain Until Date and, optional, Legal Hold status.
  - If custom metadata is added or modified for a record, a new version is automatically created as a result.
  - However, a new record version is not created as a result of extending the Retain Until Date or modifying the Legal Hold attribute.
- The following retention controls may be (a) transmitted with a record or (b) set via the application of Bucket default values:
  - *Object Locking* mode, set to *Compliance, Governance* or *Null*. **Only *Compliance* mode meets the strict requirements of the SEC Rule 17a-4(f) to preserve a record in a non-rewriteable, non-erasable format.**
  - Retain Until Date, set to a date in the future.

Note: The Retention controls listed above must be set ***as pairs*** *(i.e., if an Object Locking mode is set, a Retain Until Date must also be set). For objects uploaded via the Wasabi Management Console, Bucket defaults are applied.* If Bucket defaults do not exist, the uploaded objects are stored ***without retention controls***. *Further, if* *the Retain Until Date (transmitted or calculated using the default) is outside the allowed Min/Max range, the recording process fails and an error message is issued.*

- Multiple *Object Locking* modes are supported within a given Bucket. This means that a single Bucket, with the *Object Locking* feature enabled, may contain a mixture of objects that are (a) locked with *Compliance* mode, (b) locked with *Governance* mode, or (c) remain unlocked.
- Authorized users may extend the Retain Until Date for a record, as needed.
- A Record version with an *Object Locking* mode of *Compliance*:
  - May not be moved to another folder within the same Bucket, nor to another Bucket until past its Retain Until Date.
  - May be copied to another folder within the same Bucket or to another Bucket, however, no retention controls are carried with the copy. The new copy is assigned a unique record ID and must have its own retention controls applied (i.e., *Object Locking* mode, Retain Until Date and Legal Hold attribute). The original record remains unchanged. This process of copying and applying retention controls is performed separately for each version, as needed.
- When litigation or a subpoena requires objects to be placed on hold, which could entail retaining them beyond their assigned retention period, the regulated entity must ensure the subject objects are protected for the duration of the legal hold by applying a Legal Hold (Y) attribute (a.k.a., temporary hold). A Legal Hold (Y) attribute:
  - May be applied to any object version stored (with or without applied retention controls) in a Bucket that has the *Object Locking* feature enabled.
  - May be included with the initial transmission of the object to the target storage Bucket as an additional retention control attribute, or authorized users may set the Legal Hold attribute on previously stored object versions via the *Put Legal Hold* S3 API.
  - Can be removed from the object versions when no longer required. Thereafter, immutability controls are once again governed by any retention controls applied to the object version.
- While subject to a *Hold*:
  - New versions of an object may be created; however, a Legal Hold must be set separately for each new version.
  - An object version, including custom metadata, cannot be modified, overwritten or deleted by any means, even if its Retain Until Date has passed.
  - The Retain Until Date for an object may be extended, however, the new date will not take effect until the Legal Hold is removed.
- The following chart illustrates the integrated controls that are applied to records during the storage process, based on (a) the retention controls transmitted with the record, (b) the default values configured for the target storage Bucket, and (c) any transmitted Retain Until Date meeting the Min/Max guardrails set through an IAM policy. (As a reminder, if the Retain Until Date is outside user's allowable Min/Max range, the recording process fails and an error message is issued.)

Transmitted Object Locking Mode	**Transmitted Retain Until Date**	**Transmitted Legal Hold**	**Action if Bucket has NO default settings**	**Action if Bucket has a PAIR of defaults (*Object Locking* Mode and Retention Period)**
Null/None	None	Null or No	Stored without retention controls: ● The object is immutable. ● Any changes or overwrites of the object results in a new version. ● Object may be deleted. ● No retention is applied to the object. ● No legal hold attribute is applied.	Stored with default retention controls: ● The object is immutable. ● Any changes or overwrites of the object results in a new version. ● The Bucket’s default Object Locking mode is assigned. ● Retain Until Date is calculated using the creation/storage date plus the default Retention Period. ● No Legal Hold attribute is applied.
Null/None	None	Yes	Stored with legal hold controls: ● The object is immutable. ● Any changes or overwrites of the object results in a new version. ● No retention is applied to the object. ● Legal Hold attribute is applied, which prevents object from deletion indefinitely until Legal Hold is removed.	Stored with default retention controls: ● The object is immutable. ● Any changes or overwrites of the object results in a new version. ● The Bucket’s default mode is assigned. ● Retain Until Date is calculated using the creation/storage date plus the default Retention Period. ● Legal Hold attribute is applied, which overrides deletion eligibility, based on the Retain Until Date, and prevents deletion indefinitely until Legal Hold is removed.
Null/None	mm/dd/yyyy	Null or No	Storage is rejected; an *Object Locking* Mode must be transmitted with a Retain Until Date.	
Null/None	mm/dd/yyyy	Yes	Storage is rejected; an *Object Locking* Mode must be transmitted with a Retain Until Date.	
Governance	None	Null or No	Storage is rejected; an *Object Locking* Mode must be transmitted with a Retain Until Date.	
Governance	None	Yes	Storage is rejected; an *Object Locking* Mode must be transmitted with a Retain Until Date.	
Governance	mm/dd/yyyy	Null or No	Stored with transmitted retention controls: ● The object is immutable. ● Any changes or overwrites of the object results in a new version. ● Governance mode is assigned. ● Retain Until Date is set to mm/dd/yyyy. ● ***The S3 Bypass WORM API may be used to remove both the Object Locking mode and the Retain Until Date***. ● No Legal Hold attribute is applied.	
Governance	mm/dd/yyyy	Yes	Stored with transmitted retention controls: ● The object is immutable. ● Any changes or overwrites of the object results in a new version. ● Governance mode is assigned.	

Transmitted Object Locking Mode	Transmitted Retain Until Date	Transmitted Legal Hold	Action if Bucket has NO default settings	Action if Bucket has a PAIR of defaults (*Object Locking* Mode and Retention Period)
			● Retain Until Date is set to mm/dd/yyyy. ● ***The S3 Bypass WORM API may be used to remove both the Object Locking mode and the Retain Until Date***. ● Legal Hold attribute is applied, which overrides the Retain Until Date and prevents deletion and overrides indefinitely until Legal Hold is removed.	
Compliance	None	Null or No	Storage is rejected; an *Object Locking* Mode must be transmitted with a Retain Until Date.	
Compliance	None	Yes	Storage is rejected; an *Object Locking* Mode must be transmitted with a Retain Until Date.	
Compliance	mm/dd/yyyy	Null or No	Stored with transmitted retention controls: ● The object is immutable. ● Any changes or overwrites of the object results in a new version. ● Object Locking mode of *Compliance* is assigned and cannot be modified or removed. ● Retain Until Date is set to mm/dd/yyyy and cannot be shortened or removed, only extended if needed. NOTE: Extending the Retain Until Date does <u>not</u> cause a new version to be created. ● No Legal Hold attribute is applied.	
Compliance	mm/dd/yyyy	Yes	Stored with transmitted retention controls: ● The object is immutable. ● Any changes or overwrites of the object results in a new version. ● *Object Locking* mode of *Compliance* is assigned and cannot be modified or removed. ● Retain Until Date is set to mm/dd/yyyy and cannot be shortened or removed, only extended if needed. NOTE: Extending the Retain Until Date does <u>not</u> cause a new version to be created. ● Legal Hold attribute is applied, which overrides deletion eligibility, based on the Retain Until Date and prevents deletion and overrides indefinitely, until the Legal Hold is removed.	

2.2.3.4 Deletion Controls

- Record versions are eligible for deletion when the following conditions are met:
  - The applied Retain Until Date is in the past, and
  - The Legal Hold attribute is set to N or Null.
- Authorized users may delete <u>eligible</u> records (and any replicas) directly from the Wasabi console or via the S3 Delete Object API.
  - If a specific *version* of a record is deleted, it is removed from storage.
  - If a record is deleted, without specifying a version, a delete marker is added as the top version for that object.

  - Lifecycle policies are currently not supported in Wasabi Hot Cloud Storage; however, the use of custom scripting is supported.

- Buckets with *Object Locking* enabled may only be deleted if empty.

- Similar to decommissioning hardware that is on-premises, the regulated entity's account, along with all Buckets and records, *can be deleted by the regulated entity's root user account*. Multi-factor authentication (MFA) must be used to help protect against unauthorized malicious root administrator actions.

2.2.3.5 Security

In addition to the stringent retention protection and management controls described above, Wasabi provides the following security capabilities, which support the authenticity and reliability of the records.

- The Wasabi Hot Cloud Storage data centers are certified for SOC 2 and ISO 27001.

- Access capabilities that are supported include: multi-factor authentication (MFA), enterprise single sign-on (SSO), and identity and access management (IAM) policies that apply *roles* to users and groups.

- Access Keys, combined with Secret Access Keys, are used by third party applications to make secure REST protocol requests to Wasabi Hot Cloud Storage.

- Wasabi Hot Cloud Storage supports encryption of records and associated metadata as follows:

  - Data is automatically encrypted while in transit, via HTTPS.

  - Data-at-rest-encryption (DARE) is always performed during the write process, using an AES256-bit encryption key that is provided in one of the following ways:

    - Server-Side Encryption with Customer-Provided Keys (SSE-C) – The regulated entity manages its own encryption keys; Wasabi never stores the encryption keys.

    - Server-side Encryption with Wasabi-Managed Keys – Wasabi generates a unique encryption key for each object during the write process and stores the key in the secure metadata layer of the Wasabi system.

2.2.3.6 Clock Management

- To protect against the possibility of the premature deletion of objects, Wasabi synchronizes all system clocks in the Wasabi Hot Cloud Storage environment with an external NTP source.

- Wasabi system clocks regularly and frequently check the time of the external source and if there is a small time drift, automatically resynchronizes to the external source time. If a large drift is detected, administrators are alerted and manual intervention by the administrator is required.

  - MFA is required for the administrator to modify any system clock.

  - The administrator's action is logged in the Wasabi logging system.

2.2.4 Additional Considerations

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

- Enabling *versioning* and the *Object Locking* feature for Buckets intended to store required records in compliance with the SEC Rule 17a-4(f).
- Appropriately assigning privileges to users or groups who are responsible for managing retention controls within the Wasabi Hot Cloud Storage environment.
- Transmitting a pair of explicit retention controls with each record (i.e., *Object Locking* mode of *Compliance* and a Retain Until Date) to be applied during the recording process.
  - Cohasset recommends establishing the following Bucket-level defaults: (a) *Object Locking* mode of *Compliance* and (b) an appropriate default retention period, to ensure that records transmitted without explicit retention controls, including those uploaded via Wasabi Management Console capabilities, are immutably protected for the default retention period.
  - Cohasset additionally recommends assigning Min/Max retention values to users or groups through IAM policies, to act as guardrails, ensuring appropriate Retain Until Dates are applied to records.
- Storing records requiring event-based[11] retention periods in a separate compliance system, since Wasabi Hot Cloud Storage does not currently support event-based retention periods.
- Applying Legal Holds to object versions that require preservation for legal matters, government investigations, external audits and other similar circumstances, and removing the Legal Holds when the applicable action is completed.
- Extending Retain Until Dates as required on record versions.
- Specifying the VersionID for delete requests, which prevents delete markers from inhibiting searchability.
- Maintaining any SSE-C encryption keys used during the recording process to assure continued access to stored records.
- Maintaining Access Keys and Secret Access Keys used by third party applications for secure REST protocol access to the Wasabi system.
- Establishing policies and procedures to regularly monitor system error messages (e.g., storage rejections notices, system clock adjustments) and take immediate corrective action.
- Procedurally requiring the use of MFA for root user access and monitoring activities of these privileged accounts.

Additionally, the regulated entity is responsible for (a) maintaining their Wasabi account in good standing and paying for appropriate services to allow records to be retained until the applied retention periods and holds have expired or until the records have been transferred to another compliant storage system, (b) authorizing user privileges, and (c) maintaining appropriate hardware and software, encryption keys, and other information and services needed to retain the records.

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

2.3 Record Storage Verification

2.3.1 Compliance Requirement

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.

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

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

2.3.3 Wasabi Hot Cloud Storage Capabilities

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

2.3.3.1 Recording Process

- An MD5 hash value is required to be transmitted from the source system with every object. Wasabi calculates its own hash value for the object and compares it to the transmitted hash value. If the two values are the same, the object is recorded and the hash value stored as metadata for the object.
- Wasabi utilizes a custom data storage structure, similar to RAID, for recording objects. Objects are divided into fragments and are distributed with parity bits across different storage units during the write process to ensure data durability. Wasabi Hot Cloud Storage asserts 99.999999999% (11-nines) of durability.

2.3.3.2 Post-Recording Verification Process

- To validate continued data integrity, Wasabi regularly performs scans of data at rest to verity that no data corruption has occurred. Should corruption be detected, parity bits are utilized to recreate the object from the remaining fragments.
- During retrieval of an object, Wasabi recalculates the hash value for the object and compares it to the hash value stored at the time of recording. If the hash values are not equal, an error is returned and manual corrective action is required by the Wasabi Hot Cloud Storage administrator.

2.3.4 Additional Considerations

- The source system is responsible for transmitting the complete contents of the required record.
- Cohasset recommends utilizing HTTPS (a secure internet transfer protocol), when practical, to reduce the chance of network-level errors when transmitting and inputting the records.

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 either a:

- Human readable format that can be naturally read by an individual, or
- 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 Audit-Trail*.

2.4.2 Compliance Assessment

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

2.4.3 Wasabi Hot Cloud Storage Capabilities

The following capabilities relate to the requirement for capacity to download and transfer records and the information needed to locate the records.

- Wasabi Hot Cloud Storage assures each record is assigned a unique ID comprised of the following attributes:
  - **Object Key** - which includes the Bucket Name, folder name, and file name.
  - **Version ID -** a new version ID is assigned when (a) an object with the same object key is uploaded or (b) when an object is replicated using WCSM replication.

  Both the Object Key and Version ID are immutably stored as metadata for the record for the duration of the retention period.
- The creation/storage timestamp (cdate) is captured and immutably stored with each record for the duration of the retention period.
- Authorized users can search the contents of a Bucket via the S3 LIST OBJECT APIs, to produce the following results:
  - List the top (active) version of all records contained in the Bucket.
  - Filter the list of records in the Bucket by prefix, such as folder name or filename.

  Notes:

  - List results will include system metadata but will not include retention attributes such as Retain Until Date or *Object Locking* mode.

    - Additionally, if the top version of a record is a delete marker, that record will not be included in the List results. If the delete marker is removed, the top version of the record will be included in List results.

- The GET-OBJECT API may be utilized to return the record:
  - When the request includes the version identifier, the specific record version is returned.
  - When no version identifier is specified, the most recent version is returned, unless the most recent version is a delete marker, in which case an error code is returned.
- The GET-OBJECT-RETENTION API may be utilized to obtain retention attributes associated with an individual record version.
- Once records are located, they may be downloaded in one of the following ways:
  - Using the Wasabi console, desired records can be selected for download. Objects are downloaded as individual files (i.e., not zipped) but associated metadata is not included.
    - When a version ID is specified, the specific version is downloaded.
    - If no version ID is specified, the top (active) version is downloaded. Note: If the top (active version) of a record is a delete marker, the record is not downloaded.
  - The source system can be used to download the selected records.
  - S3-compatible APIs may be used to download one or more records and associated metadata (including retention attributes).

2.4.4 Additional Considerations

In addition, for this requirement, the regulated entity is responsible for: (a) maintaining its account in good standing, (b) authorizing user privileges, (c) maintaining appropriate hardware and software capacity, encryption keys, and other information and services needed to use Wasabi Hot Cloud Storage to readily access, download, and transfer the records and the information needed to locate the records, and (d) providing requested information to the regulator, in the requested format.

2.5 Record Redundancy

2.5.1 Compliance Requirement

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

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

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

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

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

- The intent of paragraph (A) is:

  [B]ackup electronic recordkeeping system must serve as a redundant set of records if the original electronic recordkeeping system is temporarily or permanently inaccessible because, for example, it is impacted by a natural disaster or a power outage.[12] [emphasis added]

- The intent of paragraph (B) is:

  [R]edundancy capabilities that are designed to ensure access to Broker-Dealer Regulatory Records or the SBS Entity Regulatory Records must have a level of redundancy that is at least equal to the level that is achieved through using a backup recordkeeping system.[13] [emphasis added]

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

2.5.2 Compliance Assessment

Cohasset asserts that the functionality of Wasabi Hot Cloud Storage meets this requirement in SEC Rules 17a-4(f)(2)(v)(B) and 18a-6(f)(2)(v)(B) by retaining a persistent alternate source to reestablish the records through the use of erasure coding, when the considerations described in Section 2.5.4 are satisfied.

2.5.3 Wasabi Hot Cloud Storage Capabilities

For compliance with paragraph (B), Wasabi Hot Cloud Storage uses erasure coding (EC) to redundantly store data blocks of records. In the event of a disk failure, the original record can be regenerated.

- Wasabi storage is designed to provide 99.999999999% (11-nines) durability and high availability of objects over a given year, as defined in their service level agreement.
  - Data is recorded in the Wasabi Hot Cloud Storage environment using advanced erasure coding algorithms. Objects are written in a series of data and parity fragments and distributed across multiple drives that are located in different power and network domains (i.e., Wasabi storage slices, pods, and vaults).
  - In the event of drive failure, storage server failure, or data corruption, records can be accurately *regenerated* from the erasure coded data.
- Optionally, the source system may serially record each record into two or more separate storage regions to achieve geographically dispersed duplication. Management of duplicate records created in this manner must be handled by the source system.

2.5.4 Additional Considerations

In addition, for this requirement, the regulated entity is responsible for: (a) maintaining its account in good standing, (b) maintaining the technology, storage capacity, encryption keys, and other information and services needed to use Wasabi Hot Cloud Storage.

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

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

2.6 Audit System

2.6.1 Compliance Requirement

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

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

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

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

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

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

2.6.2 Compliance Assessment

Cohasset asserts that Wasabi Hot Cloud Storage supports the regulated entity's efforts to meet this SEC audit system requirement.

2.6.3 Wasabi Hot Cloud Storage Capabilities

The regulated entity is responsible for an audit system and compliance is supported by Wasabi Hot Cloud Storage.

- When inputting files, Wasabi Hot Cloud Storage applies a unique identifier (a combination of Object Key and Version ID) and a system-generated creation/storage timestamp. These attributes are immutably stored as record metadata for the duration of the retention period and provide accountability related to the inputting of records.
- Each record is immutably stored for the duration of the retention period; therefore, no changes are allowed once the record is stored.
- In addition to the immutable record metadata and content, Wasabi Hot Cloud Storage offers a Bucket logging feature. When logging is enabled for a Bucket, a text log file is created which provides a record of all access to the bucket, including PutObject and DeleteObject operations. Details contained in the log file include the type of request, resources specified in the request, and the timestamp that the request was processed.
  - Bucket log files should be stored in a separate Bucket that is dedicated to log files, with appropriate retention applied, or alternatively, exported to a third-party audit system for long term retention.
  - Bucket log files may be downloaded to a local system and viewed with a Wasabi Bucket Logs Viewer tool.

2.6.4 Additional Considerations

The regulated entity is responsible for maintaining an audit system for inputting records and may utilize Wasabi Hot Cloud Storage features alone or in conjunction with another system.

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

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

The focus of 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 audit-trail and (2) non-rewriteable, non-erasable, a.k.a. WORM, are more likely to achieve this objective because each alternative requires the specific and testable outcome of accessing and producing modified or deleted records, in their original form, for the required retention period.

> *The proposed amendments to Rules 17a-4 and 18a-6 and the [CFTC] principles-based approach recommended by the commenters share an objective: ensuring the authenticity and reliability of regulatory records. However, the audit-trail requirement is more likely to achieve this objective because, like the existing WORM requirement, it sets forth a specific and testable outcome that the electronic recordkeeping system must achieve: the ability to access and produce modified or deleted records in their original form.*[14] [emphasis added]

The focus of Cohasset's assessment, in Section 2, pertains to Wasabi Hot Cloud Storage, with the *Object Locking* feature in *Compliance* mode, which is a highly restrictive configuration that assures the storage solution applies integrated controls to (a) protect immutability of the record content and certain system metadata and (b) prevent deletion over the applied retention period. Additionally, in subsection 2.2.3.3, *Records, Retention Controls and Legal Holds*, Cohasset compares the integrated control codes of the *Object Locking* feature in the highly-restrictive *Compliance* mode to the less-restrictive *Governance* mode.

In the following table, Cohasset correlates the functionality of Wasabi Hot Cloud Storage, using the *Object Locking* feature in *Compliance* mode, with the *principles-based* CFTC requirements related to the *form and manner of retention* and the *inspection and production of regulatory records*. In addition, Cohasset contends that Wasabi Hot Cloud Storage, using the less restrictive *Governance mode,* meets these *principles-based* CFTC requirements, when the regulated entity applies appropriate procedural controls to oversee operations that may allow content to be modified or deleted prior to expiration of the retention period. This less restrictive *Governance* mode provides flexibility to remove or shorten retention periods, which may be beneficial for compliance with privacy and data protection requirements. The first column enumerates the CFTC regulation. The second column provides Cohasset's analysis and opinion regarding the ability of Wasabi Hot Cloud Storage to meet the requirements for electronic regulatory records in CFTC Rule 1.31(c)-(d).

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

CFTC 1.31(c)-(d) Regulation [emphasis added]	**Compliance Assessment Relative to CFTC 1.31(c)-(d)**
(c) Form and manner of retention. Unless specified elsewhere in the Act or Commission regulations in this chapter, all regulatory records must be created and retained by a records entity in accordance with the following requirements: *(1) Generally. Each records entity shall retain regulatory records in a form and manner that ensures the authenticity and reliability of such regulatory records in accordance with the Act and Commission regulations in this chapter.* *(2) Electronic regulatory records. Each records entity maintaining electronic regulatory records shall establish appropriate systems and controls that ensure the authenticity and reliability of electronic regulatory records, including, without limitation:* *(i) Systems that maintain the security, signature, and data as necessary to ensure the authenticity of the information contained in electronic regulatory records and to monitor compliance with the Act and Commission regulations in this chapter;*	It is Cohasset's opinion that the CFTC requirements in (c)(1) and (c)(2)(i), for records[15] with time-based retention periods, are met by the functionality of Wasabi Hot Cloud Storage, with the *Object Locking* feature in *Compliance* or *Governance* mode. This report describes the functionality of Wasabi Hot Cloud Storage, with the *Object Locking* feature in *Compliance* mode in: ● Section 2.2, *Non-Rewriteable, Non-Erasable Record Format* ● Section 2.3, *Record Storage Verification* ● Section 2.4, *Capacity to Download and Transfer Records and Location Information* ● Section 2.6, *Audit System* Additionally, for *records stored electronically*, the CFTC definition of *regulatory records* in 17 CFR § 1.31(a) includes information to access, search and display records, as well as data on records creation, formatting and modification: *Regulatory records means all books and records required to be kept by the Act or Commission regulations in this chapter, including any record of any correction or other amendment to such books and records, provided that, with respect to such books and records stored electronically, regulatory records shall also include:* *(i) Any data necessary to access, search, or display any such books and records; and* *(ii) All data produced and stored electronically describing how and when such books and records were created, formatted, or modified.* [emphasis added] Wasabi Hot Cloud Storage retains immutable metadata attributes as an integral component of the records, and, therefore, these attributes are subject to the same retention protections 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. The immutable metadata attributes include the following: ● Object Key (Bucket name, folder name, filename), ● Version ID, ● Creation/storage date/time, and ● Object Locking mode (which is immutable, if set to Compliance). Additionally, mutable metadata attributes stored for records include retention controls and legal hold statuses. The most recent values of mutable metadata are retained for the same time period as the associated records. Further, Wasabi Hot Cloud Storage in conjunction with the Bucket Logging feature 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 2.6, *Audit System*.

[15] If Wasabi Hot Cloud Storage retains the regulatory record content and core metadata attributes but does not necessarily retain other information needed to satisfy this definition of a regulatory record (such as information to augment search and data on how and when the records were created, formatted, or modified), the regulated entity is responsible for retaining and managing this other information 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 Wasabi Hot Cloud Storage capabilities described in Section 2.5, *Record Redundancy*, including methods for a persistent 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*.
(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 Wasabi Hot Cloud Storage has features that support the regulated entity's efforts to comply with requests for inspection and production of records, as described in. ● Section 2.2, *Non-Rewriteable, Non-Erasable Record Format* ● Section 2.4, *Capacity to Download and Transfer Records and Location Information* ● Section 2.6, *Audit System*

4 • Conclusions

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

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

- Retains records and immutable metadata attributes in non-rewriteable, non-erasable format for time-based retention periods when the *Object Locking* mode is set to Compliance and a Retain Until Date is applied.
- Prohibits deletion of a record and its immutable metadata until the applied Retain Until Date for the record is in the past.
- Permits the extension of an applied Retain Until Date to retain records for regulatory compliance.
- Allows a Legal Hold status to be applied to records subject to preservation requirements, which immutably retains the record version and prohibits deletion or overwrites until the Legal Hold attribute is removed.
- Verifies the accuracy of the process of storing and retaining records, through the use of MD5 hash values.
- Provides authorized users with the capacity and tools to access records and associated metadata with Amazon S3-compatible APIs, the Wasabi Hot Cloud Storage Management Console, or via integrated third-party applications for local reproduction and transfer, in the requested format.
- Utilizes advanced erasure coding for recording objects, which provides the ability to accurately regenerate records in the event of drive failure, storage server failure, or data corruption. Wasabi Hot Cloud Storage asserts 11-nines of durability.
- Supports the regulated entity's obligation to retain an audit system for non-rewriteable, non-erasable records.

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

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

5 • Overview of Relevant Electronic Records Requirements

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

5.1 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.

On October 12, 2022, the U.S. Securities and Exchange Commission (SEC) adopted amendments[17] to 17 CFR § 240.17a-4 (Rule 17a-4) and 17 CFR § 240.18a-6 (Rule 18a-6), which define more technology-neutral requirements for electronic recordkeeping systems.

> *The objective is to prescribe rules that remain workable as record maintenance and preservation technologies evolve over time but also to set forth requirements designed to ensure that broker-dealers and SBS Entities maintain and preserve records in a manner that promotes their integrity, authenticity, and accessibility.*[18] [emphasis added]

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

> *Under the final amendments, broker-dealers and nonbank SBS Entities have the flexibility to preserve all of their electronic Broker-Dealer Regulatory Records or SBS Entity Regulatory Records either by: (1) using an electronic recordkeeping system that meets either the audit-trail requirement or the WORM requirement; or (2) preserving some electronic records using an electronic recordkeeping system that meets the audit-trail requirement and preserving other electronic records using an electronic recordkeeping system that meets the WORM requirement.*[19] [emphasis added]

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

5.1.1 Record Audit-Trail Alternative

The objective of the record audit-trail requirement is to allow regulated entities to keep required records on business-purpose recordkeeping systems.

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

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

[19] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66419.

> *[T]o preserve Broker-Dealer Regulatory Records and SBS Regulatory Records, respectively, on the same electronic recordkeeping system they use for business purposes, but also to require that the system have the capacity to recreate an original record if it is modified or deleted. This requirement was designed to provide the same level of protection as the WORM requirement, which prevents records from being altered, over-written, or erased.*[20] [emphasis added]

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

> *[L]ike the existing WORM requirement, [the audit-trail requirement] sets forth a specific and testable outcome that the electronic recordkeeping system must achieve: the ability to access and produce modified or deleted records in their original form.*[21] [emphasis added]

Further, the audit-trail applies only to required records: *"the audit-trail requirement applies to the final records required pursuant to the rules, rather than to drafts or iterations of records that would not otherwise be required to be maintained and preserved under Rules 17a-3 and 17a-4 or Rules 18a-5 and 18a-6."*[22] [emphasis added]

5.1.2 Non-Rewriteable, Non-Erasable Record Format Alternative

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

> *The Commission confirms that a broker-dealer or nonbank SBS Entity can rely on the 2003 and 2019 interpretations with respect to meeting the WORM requirement of Rule 17a-4(f) or 18a- 6(e), as amended.*
> *****
> *In 2001, the Commission issued guidance that Rule 17a-4(f) was consistent with the ESIGN Act. The final amendments to Rule 17a-4(f) do not alter the rule in a way that would change this guidance. Moreover, because Rule 18a-6(e) is closely modelled on Rule 17a-4(f), it also is consistent with the ESIGN Act****[23] [emphasis added]

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

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

[20] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.

[21] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.

[22] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66418.

[23] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66419.

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

> *A broker-dealer would not violate the requirement in paragraph* [(f)(2)(i)(B) (refreshed citation number)] *of the rule if it used an electronic storage system that prevents the overwriting, erasing or otherwise altering of a record during its required retention period through the use of integrated hardware and software control codes.*[24] [emphasis added]

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

> *The Commission is clarifying that a software solution that prevents the overwriting, erasing, or otherwise altering of a record during its required retention period would meet the requirements of the rule.*[25] [emphasis added]

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

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

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

> *[A] broker-dealer must take appropriate steps to ensure that records are not deleted during periods when the regulatory retention period has lapsed but other legal requirements mandate that the records continue to be maintained, and the broker-dealer's storage system must allow records to be retained beyond the retentions periods specified in Commission rules.*[26] [emphasis added]

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

5.2 Overview of FINRA Rule 4511(c) Electronic Recordkeeping System Requirements

Financial Industry Regulatory Authority (FINRA) rules regulate member brokerage firms and exchange markets. Additionally, FINRA adopted amendments clarifying the application of FINRA rules to security-based swaps (SBS).[27]

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

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

[24] 2003 Interpretative Release, 68 FR 25282.

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

[26] 2003 Interpretative Release, 68 FR 25283.

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

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

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

> *Consistent with the Commission's emphasis on a less-prescriptive, principles-based approach, proposed § 1.31(d)(1) would rephrase the existing requirements in the form of a general standard for each records entity to retain all regulatory records in a form and manner necessary to ensure the records' and recordkeeping systems' authenticity and reliability.*[28] [emphasis added]

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

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

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

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

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

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

6 • Cloud Provider Undertaking

6.1 Compliance Requirement

Separate from the electronic recordkeeping system requirements described in Section 2, Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e), the SEC requires submission of an undertaking when records are stored 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 can (a) independently access the records, (b) allow regulators to examine the records, during business hours, and (c) promptly furnish the regulator with true, correct, complete and current hard copy of the records.

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

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

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

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

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

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

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

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

> *representative or designee or SIPA trustee the same type of technical support with respect to records access that it would provide to the broker-dealer or SBS Entity in the normal course.*[29] [emphasis added]

6.2 Wasabi Undertaking Process

- The undertaking requires actions be taken by both parties:
  1. The regulated entity affirms 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 Wasabi Hot Cloud Storage, and
     - Consents to Wasabi fulfilling the obligations set forth in this undertaking.
  2. Wasabi:
     - 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 submits the undertaking to the SEC.
- IMPORTANT NOTE: While Wasabi provides this undertaking to the SEC on behalf of the regulated entity, the regulated entity is not relieved from its responsibility to prepare and maintain required records.

6.3 Additional Considerations

The regulated entity is responsible for (a) initiating the undertaking, (b) maintaining its account in good standing, (c) maintaining hardware and software, encryption keys and privileges to access Wasabi Hot Cloud Storage, and (d) assuring that the regulator has (when needed) access privileges, encryption keys, and other information and services to permit records to be accessed, downloaded, and transferred.

[29] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66429.

About Cohasset Associates, Inc.

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

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

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

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

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

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

For domestic and international clients, Cohasset:

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

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